

HiPath Wireless Standalone Access Point, V1.0

Bedienungsanleitung

SIEMENS

Global network of innovation

1P A31003-W1110-U100-4-19

Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden. Die verwendeten Marken sind Eigentum der Siemens AG bzw. der jeweiligen Inhaber.

© Siemens AG 2007 • Siemens Communications,
Hofmannstraße 51, D-81359 München
Bestell-Nr.: A31003-W1110-U100-4-19
Liefermöglichkeiten und technische Änderungen vorbehalten.

Inhalt

1 Willkommen 5
1.1 Informationen zu dieser Bedienungsanleitung 5
1.2 Informationen zum Handbuch Erste Schritte 5
1.3 An wen richtet sich diese Bedienungsanleitung? 6
1.4 Kapitelübersicht 6
1.5 Referenzdokumente 7
1.6 Formatierungskonventionen 7
1.7 Paketinhalt 8

2 Rechtliche Bestimmungen 9
2.1 AP2630 mit interner Antenne, AP2640 mit externer Antenne 10
2.1.1 USA - Erklärung zur Konformität mit den Vorschriften der Federal Communications Commission (FCC) 11
2.1.2 Kanada - Department of Communications Compliance Statement 19
2.1.3 Europäische Union 26
2.1.4 Zertifizierungen anderer Länder 38
2.2 Liste der länderspezifischen Unterstützung 39

3 Info zum HiPath Wireless Standalone Access Point 45
3.1 Funktionsweise konventioneller drahtloser LANs 45
3.2 Funktionsweise des Standalone Access Point 46
3.3 Standalone Access Point und Ihr Netzwerk 46
3.3.1 Standalone Access Point-Netzwerkkomponenten 46
3.3.2 Info zur Netzwerksicherheit 47
3.3.3 Info zu Quality of Service (QoS) 48
3.4 Info zu Clustering 48
3.4.1 Bilden eines Clusters 48

4 Installieren und Konfigurieren des Standalone Access Point 51
4.1 Installieren des Standalone Access Point 51
4.2 Anschlüsse und Stromversorgung für den Standalone Access Point 52
4.3 Erklärung des LED-Status für den Standalone Access Point 53
4.4 Wiederherstellen der werkseitigen Standardeinstellungen 54

5 Erste Schritte mit dem Standalone Access Point 57
5.1 Benutzeroberfläche 57
5.2 Anmelden am Standalone Access Point 58
5.3 Ändern von Kennwörtern 60
5.4 Herunterladen der Firmware 61
5.5 Einstellen der Oberflächensprache 63
5.6 Ändern der Host-IP-Adresse 64
5.7 Zugreifen auf die Hilfefunktion 65

6 Konfigurieren des Standalone Access Point 67
6.1 Konfigurieren der LAN-Einstellungen 67
6.2 Konfigurieren der WLAN-Einstellungen 71
6.2.1 Konfigurieren der WLAN-Basiseinstellungen 71
6.2.2 Konfigurieren der WLAN-Filtereinstellungen 73
6.2.3 Konfigurieren der erweiterten 802.11b/g-Einstellungen 74
6.2.4 Konfigurieren der erweiterten 802.11a-Einstellungen 79
6.2.5 Konfigurieren der WLAN-QoS-Einstellungen 82
6.3 Konfigurieren von VNS für den Standalone Access Point 84
6.3.1 Einrichten der allgemeinen VNS-Konfiguration 84
6.3.2 Konfigurieren von Einstellungen für die VNS-Funkfrequenz 86
6.3.3 Konfigurieren von VNS-Sicherheitseinstellungen. 88
6.3.4 Konfigurieren von VNS-QoS-Einstellungen 91
6.4 Verwalten der Konfiguration 96
6.4.1 Speichern der Konfiguration. 96
6.4.2 Wiederherstellen der Konfiguration 97
6.4.3 Wiederherstellen der werkseitigen Standardeinstellungen. 99
6.4.4 Aktualisieren des BootROM 100

7 Problembehandlung beim Standalone Access Point. 103
7.1 Neustart. 103
7.2 Anzeigen von Systemstatus-Informationen. 104
7.3 Anzeigen von Protokollstatus-Informationen. 105
7.4 Anzeigen von LAN-Status-Informationen 107
7.5 Anzeigen von 802.11b/g-Statusinformationen 108
7.6 Anzeigen von 802.11a-Statusinformationen. 109
7.7 Anzeigen von Informationen zum Client-Status 111
7.8 Anzeigen von Informationen zum Cluster-Status 112

8 Konvertieren von Access Points 115
8.1 Konvertieren eines Standalone Access Point 2630/2640 in einen Access Point 2610/2620 115
8.2 Konvertieren eines Access Point 2610/2620 in einen Standalone Access Point 2630/2640 115

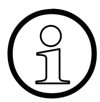
9 Glossar: Netzwerk-Begriffe und -Abkürzungen 119

A Anhang: Protokollcodes und -meldungen 137

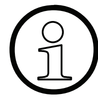
B Anhang: Unterstützte Standards 139
B.1 RFC-Liste 139
B.2 Liste der 802.11-Standards 140

1 Willkommen

Diese Bedienungsanleitung enthält Hinweise für die Installation und Konfiguration des HiPath Wireless Standalone Access Point.



Lesen Sie bitte die folgenden Sicherheitshinweise und das Handbuch *HiPath Wireless Standalone Access Point, Erste Schritte* vor der Erstverwendung vollständig durch. Stellen Sie auch sicher, dass Kinder, die Zugang zum HiPath Wireless Standalone Access Point haben, diese Sicherheitshinweise kennen.



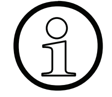
Lesen Sie bitte die folgenden Sicherheitshinweise und die vorliegende Bedienungsanleitung vor der Erstverwendung vollständig durch. Stellen Sie auch sicher, dass Kinder, die Zugang zum HiPath Wireless Standalone Access Point haben, diese Sicherheitshinweise kennen.

- Der HiPath Wireless Standalone Access Point ist für den Einsatz im Wohn- und im Arbeitsbereich vorgesehen.
- Das Gehäuse des HiPath Wireless Standalone Access Point darf nicht geöffnet werden. Wenden Sie sich bei Problemen an autorisiertes Fachpersonal.
- Verwenden Sie ausschließlich Originalzubehör. Die Verwendung von anderem Zubehör ist gefährlich und führt zum Verlust der Gewährleistung und der Gültigkeit des CE-Kennzeichens.
- Stellen Sie sicher, dass der HiPath Wireless Standalone Access Point nicht mit Flüssigkeiten wie Tee, Kaffee, Säften oder Erfrischungsgetränken in Berührung kommt.

1.1 Informationen zu dieser Bedienungsanleitung

1.2 Informationen zum Handbuch Erste Schritte

Der Standalone Access Point ist ein WLAN Access Point, der für die Netzwerkkommunikation die 802.11-Standards (802.11a+b/g) für drahtlose lokale Netzwerke nutzt. Außerdem dient der Standalone Access Point als Bridge für den Netzverkehr in ein Ethernet-LAN. Der Standalone Access Point ist physikalisch mit einer LAN-Infrastruktur verbunden. Der Funk auf dem Standalone Access Point kann in der Benutzeroberfläche aktiviert oder deaktiviert werden.



Der Standalone Access Point kann innerhalb der in Ihrem Land verfügbaren Frequenzbereiche betrieben werden. Weitere Informationen finden Sie unter Kapitel 2, “Rechtliche Bestimmungen”.

Die *HiPath Wireless Standalone Access Point User Guide* beschreibt, wie Sie Ihren HiPath Wireless Standalone Access Point installieren, konfigurieren und verwalten.

Das Handbuch *HiPath Wireless Standalone Access Point Getting Started Guide* beschreibt, wie Sie Ihren HiPath Wireless Standalone Access Point installieren, konfigurieren und verwalten.

1.3 An wen richtet sich diese Bedienungsanleitung?

Die *HiPath Wireless Standalone Access Point User Guide* richtet sich an Installationstechniker und alle anderen Mitarbeiter im Unternehmen, die für die Installation und Konfiguration des Standalone Access Point zuständig sind.

1.4 Kapitelübersicht

Die vorliegende Bedienungsanleitung enthält folgende Kapitel:

- Kapitel 1, “Willkommen”, beschreibt die Zielgruppe und den Inhalt der Anleitung sowie die verwendeten Formatierungskonventionen.
- Kapitel 2, “Rechtliche Bestimmungen”, enthält die rechtlichen Bestimmungen für den Standalone Access Point.
- Kapitel 3, “Info zum HiPath Wireless Standalone Access Point”, bietet einen Überblick über das Produkt und beschreibt seine Leistungsmerkmale und Funktionen, einschließlich Einrichtung eines Clusters.
- Kapitel 4, “Installieren und Konfigurieren des Standalone Access Point”, beschreibt die Installation des Standalone Access Point, den Anschluss und die Stromversorgung des Geräts sowie die Funktionsweise der LED-Anzeigen und ihre Bedeutung.
- Kapitel 5, “Erste Schritte mit dem Standalone Access Point”, beschreibt die Anmeldung bei der Benutzerschnittstelle sowie weitere Prozeduren wie den Download der Firmware, das Ändern von Kennwörtern und das Aufrufen der Hilfe.
- Kapitel 6, “Konfigurieren des Standalone Access Point”, enthält Informationen zum Konfigurieren von LAN-Einstellungen, zum Speichern und Wiederherstellen von Konfigurationen und zum Aktualisieren des BootROM.
- Kapitel 7, “Problembehandlung beim Standalone Access Point”, enthält Informationen zum Neustarten des Standalone Access Point und zum Anzeigen von Statusinformationen für den Standalone Access Point.
- Kapitel 8, “Konvertieren von Access Points”, enthält Informationen zum Konvertieren von Access Points.
- Kapitel 9, “Glossar: Netzwerk-Begriffe und -Abkürzungen”, enthält ein Glossar mit der in dieser Anleitung verwendeten Industriestandard-Terminologie.

- Anhang A, “Anhang: Protokollcodes und -meldungen”, enthält eine Referenzliste der vom Standalone Access Point protokollierten Codes und Meldungen.
- Anhang B, “Anhang: Unterstützte Standards”, enthält eine Referenzliste der vom Standalone Access Point unterstützten RFCs.

1.5 Referenzdokumente

Die nachstehend aufgeführten Dokumente enthalten weitere Informationen zum HiPath Wireless Standalone Access Point:

- Die *HiPath Wireless Standalone Access Point Bedienungsanleitung*, die mit dem Standalone Access Point auf der System-CD ausgeliefert wird, beschreibt, wie Sie den HiPath Wireless Standalone Access Point installieren, konfigurieren und verwalten.
- Das Handbuch *HiPath Wireless Standalone, Erste Schritte*, das mit dem Standalone Access Point auf der System-CD ausgeliefert wird, beschreibt, wie Sie den HiPath Wireless Standalone Access Point installieren und konfigurieren.

1.6 Formatierungskonventionen

In diesem Handbuch werden folgende Formatierungskonventionen verwendet:

Fettschrift

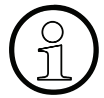
In dieser Formatierung erscheinen HiPath Wireless Standalone Access Point-Komponenten, Fenster- und Dialogfeldtitel sowie Elementnamen.

Kursivschrift

In dieser Formatierung erscheinen Verweise auf verwandte Dokumentationen.

`Nichtproportionale Schrift`

In dieser Formatierung erscheint Text, den Sie eingeben müssen oder der vom Computer in einer Meldung angezeigt wird.



Hinweise enthalten nützliche Informationen, die nicht unabdingbar sind, zum Beispiel Erinnerungen, Tipps oder Alternativmethoden zum Durchführen einer Aufgabe.



Warnungen enthalten wichtige Informationen. Das Ignorieren einer Warnung kann sich negativ auf den Betrieb der Anwendung auswirken.

1.7 Paketinhalt

Das HiPath Wireless Standalone Access Point-Paket enthält folgende Teile:

- Den Standalone Access Point
- Das Handbuch *HiPath Wireless Standalone Access Point Getting Started Guide*
- Die Standalone Access Point-Halteklammern
- Ein LAN-Ethernet-Verbindungskabel

Ein Netzgerät kann separat geordert werden. (Das Netzgerät ist erforderlich, wenn PoE nicht unterstützt wird.)

2 Rechtliche Bestimmungen



Warnungen weisen auf wichtige Informationen hin. Das Ignorieren einer Warnung kann zu Problemen mit der Anwendung führen.

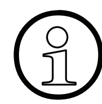
Dieses Kapitel enthält die rechtlichen Bestimmungen für den Standalone Access Point AP2630 und AP2640 (AP26XX-Serie).

Die Konfiguration der Frequenzen und der Ausgangsleistung für den Standalone Access Point wird durch die regionale Softwarelizenz und die korrekte Auswahl des Landes während der Erstinstallation und -einrichtung gesteuert. Kunden dürfen nur das Land aus ihrem lizenzierten Geltungsbereich auswählen, das ihrem geographischen Standort entspricht, um die korrekte Einrichtung von Standalone Access Points gemäß den lokalen Gesetzen und Vorschriften zu ermöglichen. Der Standalone Access Point darf erst betrieben werden, wenn er mit den korrekten Ländereinstellungen ordnungsgemäß konfiguriert wurde, da der Betrieb andernfalls lokale Gesetze und Vorschriften verletzen kann.



Am Standalone Access Point vorgenommene Änderungen, die nicht ausdrücklich durch Siemens genehmigt sind, können die Berechtigung des Benutzers zum Betreiben des Geräts ungültig machen.
Das System darf nur von autorisiertem Siemens-Servicepersonal gewartet werden. Die Prozeduren, die nur von Siemens-Personal durchgeführt werden dürfen, sind in diesem Handbuch eindeutig bezeichnet.

2.1 AP2630 mit interner Antenne, AP2640 mit externer Antenne



Der Betrieb in der Europäischen Union und anderen Ländern kann von lokalen Lizenzen, Zertifizierungen und rechtlichen Bestimmungen abhängig sein.

Optionale genehmigte externe Antennen von Drittanbietern

Der Standalone Access Point AP2640 mit externer Antenne kann auch mit optionalen externen Antennen betrieben werden, sofern diese zertifiziert sind.

Antennen-Diversität

Es gibt einige Einschränkungen für die Verwendung anderer Antennen mit Tx/Rx-Diversity:

- Wenn für Tx oder Rx die Antennen-Diversität **Best** gewählt wird, muss für die linke und die rechte Antenne dasselbe Antennenmodell verwendet werden. Wenn die externen Antennen über Kabel angeschlossen werden, müssen diese außerdem dieselbe Länge und Dämpfung haben. Wenn diese Regeln nicht eingehalten werden, funktioniert die Antennen-Diversity nicht korrekt, und es kommt in der Leistungsbilanz der Verbindung in beiden Richtungen zu Verlusten.
- Sie können sich entscheiden, nur eine Antenne zu installieren, vorausgesetzt, sowohl Tx- als auch Rx-Diversity sind darauf konfiguriert, einzig und allein diese Antenne zu verwenden. Sie können entscheiden, eine Antenne für das 11b/g-Band und eine Antenne für das 11a-Band zu installieren, vorausgesetzt, die Antennen-Diversität ist auf beiden Funkmodulen korrekt konfiguriert.

2.1.1 USA - Erklärung zur Konformität mit den Vorschriften der Federal Communications Commission (FCC)

Dieses Gerät ist konform mit Abschnitt 15 der FCC-Vorschriften. Der Betrieb unterliegt den folgenden beiden Bedingungen:

- Dieses Gerät darf keine schädlichen Störungen verursachen.
- Dieses Gerät muss alle Störungen vertragen, einschließlich Störungen, die unerwünschte Funktionen verursachen können.

Dieses Gerät wurde geprüft, und es wurde festgestellt, dass es die Grenzwerte für Digitalgeräte der Klasse B gemäß Abschnitt 15 der FCC-Vorschriften einhält. Diese Grenzwerte sind für die Gewährleistung eines angemessenen Schutzes vor schädlichen Störungen bei Installation und Betrieb im Wohn- und Arbeitsbereich gedacht. Dieses Gerät erzeugt, verwendet und emittiert Hochfrequenzenergie. Falls Sie das Gerät nicht entsprechend der Anleitung installieren oder verwenden, kann es Störungen des Rundfunkempfangs verursachen. Bei keiner Installation können Störungen jedoch völlig ausgeschlossen werden. Wenn dieses Gerät den Rundfunk- und Fernsehempfang stört, was durch Ein- und Ausschalten des Geräts festgestellt wird, kann der Benutzer versuchen, die Störung durch eine oder mehrere der folgenden Maßnahmen zu beseitigen:

- Bringen Sie die Empfangsantenne an eine andere Stelle bzw. richten Sie sie neu aus.
- Vergrößern Sie den Abstand zwischen dem Gerät und dem Empfänger.
- Schließen Sie das Gerät und den Empfänger an unterschiedliche Stromkreise an.
- Wenden Sie sich an den Händler oder einen erfahrenen Rundfunk-/TV-Techniker.

Dieses Gerät erfüllt die folgenden Konformitätsstandards:

US-amerikanische Konformitätsstandards

Sicherheit

- UL 60950-1
- UL 2043 Plenum Rated als Teil von UL 60950-1. Geeignet für die Verwendung in Luftraum-Umgebung gemäß Abschnitt 300.22.C des US National Electrical Code.

EMV

- FCC CFR 47 Abschnitt 15, Klasse B

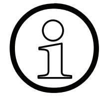
Funk-Transceiver

- FCC ID: REB-APXXX1

- CFR 47 Abschnitt 15.247, Unterabschnitt C (2,4 GHz)
- CFR 47 Abschnitt 15.407, Unterabschnitt E (5 GHz)

Sonstige

- IEEE 802.11a (5 GHz)
- IEEE 802.11b/g (2,4 GHz)
- IEEE 802.3af (PoE)



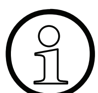
Bei der Installation des Standalone Access Point müssen die Hinweise des Herstellers genau beachtet werden, die in der vorliegenden Anleitung und in der Dokumentation des Gerätes, an das der Standalone Access Point angeschlossen wird, beschrieben werden. Eine anderweitige Installation oder Verwendung des Produkts verletzt die Bestimmungen von FCC Abschnitt 15.

Der Standalone Access Point darf nur in geschlossenen Räumen eingesetzt werden; dies gilt insbesondere für den Betrieb im UNII 5,15 - 5,25 GHz-Band gemäß 47 CFR 15.407(e).

Dieses Funkgerät gemäß Abschnitt 15 stört keine anderen auf derselben Frequenz betriebenen Geräte (NIB, Non-Interference-Basis), wenn die mitgelieferten Antennen oder andere von Siemens zertifizierte Antennen verwendet werden. Am Produkt vorgenommene Änderungen, die nicht ausdrücklich durch Siemens genehmigt sind, können die Berechtigung des Benutzers zum Betreiben des Geräts ungültig machen.

2.1.1.1 FCC-Erklärung zur Strahlenbelastung

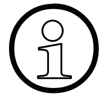
Der Standalone Access Point AP2630 und AP2640 (AP26XX-Serie) entspricht den von der FCC festgelegten Grenzwerten für die Strahlenbelastung in einer nicht kontrollierten Umgebung. Die Konformität mit den Bestimmungen zur Strahlenbelastung setzt voraus, dass sich der Endbenutzer nach der speziellen Betriebsanleitung richtet. Dieses Gerät wurde geprüft, und die Konformität wird gewährleistet bei gleichzeitigem Betrieb im 2,4 GHz- und 5 GHz-Frequenzbereich. Dieses Gerät darf nicht in der Nähe einer anderen Antenne oder eines anderen Senders aufgestellt oder zusammen mit diesen betrieben werden.



Die Ausgangsstrahlung des AP26XX Standalone Access Point liegt weit unter den von der FCC festgelegten Grenzwerten für die Strahlenbelastung gemäß Definition in "Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields" (OET Bullet 65, Supplement C). Bei der Installation und Verwendung dieses Geräts ist ein Abstand von mindestens 20 cm zwischen der Strahlungsquelle und Ihrem Körper oder anderen in der Nähe betriebenen Antennen einzuhalten.

2.1.1.2 Optionale externe Antennen von Drittanbietern

Der Standalone Access Point AP2640 kann auch mit optionalen Drittanbieter-Antennen betrieben werden, sofern diese zertifiziert sind. Möglicherweise ist jedoch eine Genehmigung durch die nationale Regulierungsbehörde erforderlich, um die Übereinstimmung mit lokalen Gesetzen und Vorschriften zu gewährleisten. Die folgenden optionalen Antennen wurden für die Verwendung mit dem Modell mit externer Antenne getestet und genehmigt.



- Bei Verwendung einer genehmigten externen Antenne eines Drittanbieters (keine Standardantenne) muss die Leistung entsprechend den nachfolgenden Tabellen eingestellt werden.
- Das Gerät muss professionell installiert werden. Für eine professionelle Installation bestehen folgende Voraussetzungen:

Vermarktung der Ausrüstung

- Das Gerät darf nicht über den Einzelhandel oder Bestellhandel an die allgemeine Öffentlichkeit verkauft werden. Es muss an Händler verkauft werden.

Professionelle Installation

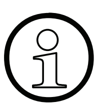
- Die Installation muss überwacht werden.
- Die Installation muss durch lizenziertes Fachpersonal erfolgen (Ausrüstung wird an Händler verkauft, die professionelles Installationspersonal beauftragen)
- Die Installation erfordert eine spezielle Schulung (spezielle Anleitung für Programmierung und Antennen- und Kabelinstallation)

Verwendung

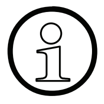
- Die Ausrüstung ist nicht zur Verwendung durch die allgemeine Öffentlichkeit vorgesehen, sondern dient zum industriellen/kommerziellen Einsatz.

#	Modell	Verwen-dung	Form	Gewinn (dBi)	Frequenz (MHz)	Koaxkabel Länge/Typ	Anschlusstyp
			Cushcraft				
#1	SR240513 5Dxxxxxx	Indoor	Gerichtet	5	2400-2500	1 Meter / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
#2	S24493DS xxxxxx	Indoor	Omni, 2 Eingänge	3	2400-2500 4900-5990	1 Meter / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 2 St.
#3	SL24513P xxxxxx	Indoor	Omni	3	2400-2500 5150-5350	1 Meter / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
#4	S24497Px xxxxx	Indoor	Gerichtet	7	2400-2500 4900-5990	1 Meter / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
			Hyperlink Tech				
#5	HG2458C Uxxx	Indoor	Omni	3	2300-2600 4900-6000	30 cm / 20AWG Coleman Cable 921021	N-Buchse
			Maxrad				
#6	MDO2400 5PTxxxxxx	Indoor	Omni, 2 Eingänge	5,2	2400-2485	1 Meter / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 2 St.

Tabelle 1 Liste der von der FCC genehmigten Antennen



Die Qualifizierungstests und -ergebnisse basieren auf den oben beschriebenen Antennen, Kabeltypen/-längen und Anschlusstypen. Weitere Kabellängen und Anschlusstypen sind verfügbar und werden durch den Suffixteil der Teilenummern angegeben (z.B. SR2405135Dxxxxxx, wobei das Suffix xxxxxx für die Kabellänge und/oder den Anschlusstyp steht). Bei den Tests wurde als Antennen-Feedline die minimale Kabellänge verwendet. Es dürfen längere Kabel verwendet werden, deren Verlust größer oder gleich den bei den Tests verwendeten Kabeln ist. Die Einstellungen für die maximale Leistung müssen gemäß diesen Tabellen erfolgen.



Wenn eine der folgenden Antennen verwendet wird, müssen Sie einen Betriebskanal (auf den Registerkarten **Erweitert 802.11b/g** und **Erweitert 802.11a**) und die entsprechende zulässige max. Leistung aus den in Tabelle 2 aufgelisteten Werten auswählen. Wählen Sie KEINEN HÖHEREN Leistungswert als den in Tabelle 2 aufgelisteten aus.

Antenne			**Antenne #1 Cushcraft SR2405135D xxxxxx**	**Antenne #2 Cushcraft S24493DS xxxxxx**	**Antenne #3 Cushcraft SL24513Pxx xxxx**	**Antenne #4 Cushcraft S24497Pxx xxxx**	**Antenne #5 Hyperlink Tech HG2458CUxx x**	**Antenne #6 Maxrad MDO24005PT xxxxxx**
	Frequenz (MHz)	Ka.-Nr.	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)
11b	2412	1	16	18	17	16	17	17
	2417	2	17	17	17	16	17	17
	2422	3	18	18	18	18	18	18
	2427	4	18	18	18	18	18	18
	2432	5	18	18	18	18	18	18
	2437	6	18	18	18	18	18	18
	2442	7	18	18	18	18	18	18
	2447	8	18	18	18	18	18	18
	2452	9	18	18	18	18	18	18
	2457	10	18	18	18	18	18	18
	2462	11	18	18	18	18	18	18

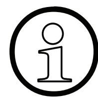
Tabelle 2 Kanal-Leistungsdaten für FCC-Antennen

Antenne			**Antenne #1 Cushcraft SR2405135D xxxxxx**	**Antenne #2 Cushcraft S24493DS xxxxxx**	**Antenne #3 Cushcraft SL24513Pxx xxxx**	**Antenne #4 Cushcraft S24497Pxx xxxx**	**Antenne #5 Hyperlink Tech HG2458CUxx x**	**Antenne #6 Maxrad MDO24005PT xxxxxx**
	Frequenz (MHz)	Ka.-Nr.	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)
11g	2412	1	10	13	13	10	12	13
	2417	2	14	15	15	14	15	14
	2422	3	15	16	16	15	16	16
	2427	4	16	18	18	16	17	17
	2432	5	16	18	18	17	18	18
	2437	6	16	18	18	17	18	18
	2442	7	18	18	18	18	18	18
	2447	8	18	18	18	18	18	18
	2452	9	18	18	18	18	18	18
	2457	10	17	17	17	17	17	18
	2462	11	14	14	14	14	14	14

Tabelle 2 Kanal-Leistungsdaten für FCC-Antennen

Antenne			Antenne #1 Cushcraft SR2405135D xxxxxx	Antenne #2 Cushcraft S24493DS xxxxxx	Antenne #3 Cushcraft SL24513Pxx xxxx	Antenne #4 Cushcraft S24497Pxx xxxx	Antenne #5 Hyperlink Tech HG2458CUxx x	Antenne #6 Maxrad MDO24005PT xxxxxx
	Frequenz (MHz)	Ka.-Nr.	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)
11a	5180	36	n. unterst.	17	17	17	17	n. unterst.
	5200	40	n. unterst.	17	17	17	17	n. unterst.
	5220	44	n. unterst.	17	17	17	17	n. unterst.
	5240	48	n. unterst.	17	17	17	17	n. unterst.
	5260	52	n. unterst.	18	18	18	18	n. unterst.
	5280	56	n. unterst.	18	18	18	18	n. unterst.
	5300	60	n. unterst.	18	18	18	18	n. unterst.
	5320	64	n. unterst.	18	18	18	18	n. unterst.
	5745	149	n. unterst.	15	n. unterst.	15	15	n. unterst.
	5765	153	n. unterst.	15	n. unterst.	15	15	n. unterst.
	5785	157	n. unterst.	14	n. unterst.	14	14	n. unterst.
	5805	161	n. unterst.	14	n. unterst.	14	14	n. unterst.
	5825	165	n. unterst.	14	n. unterst.	14	14	n. unterst.

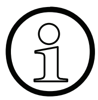
Tabelle 2 Kanal-Leistungsdaten für FCC-Antennen



Kanäle mit der Angabe "n. unterst." werden von der Antenne nicht unterstützt und dürfen auf den Registerkarten **Erweitert 802.11b/g** und **Erweitert 802.11a** nicht ausgewählt werden.



Wählen Sie bei der Antenne #3 (Cushcraft SL24513Pxxxxxx) nicht die Kanalauswahl-Option **Auto** (auf der Registerkarte **Erweitert 802.11a**) für das 11a-Funkmodul aus. Wählen Sie stattdessen nur einen Kanal aus der Liste der unterstützten Kanäle in Tabelle 2 aus.
Der Betrieb eines NICHT unterstützten Kanals ist gesetzwidrig.



Wenn Sie für die Kanalauswahl die Option **Auto** auswählen (auf den Registerkarten **Erweitert 802.11b/g** und **Erweitert 802.11a**), müssen Sie auch die in Tabelle 3 aufgelisteten Leistungswerte auswählen. Wählen Sie KEINEN HÖHEREN Leistungswert als den in Tabelle 3 aufgelisteten aus.

Antenne	11a (dBm)	11b/g (dBm)
#1	n. unterst.	10
#2	14	13
#3	17	13
#4	14	10
#5	14	12
#6	n. unterst.	13

Tabelle 3 Automatische Kanalwahl

RF-Sicherheitsabstand

Die für diesen Sender verwendeten Antennen müssen so installiert werden, dass mindestens ein Sicherheitsabstand von 20 cm zu Personen eingehalten wird, und dürfen nicht zusammen mit einer anderen Antenne oder einem anderen Sender installiert oder betrieben werden.

2.1.2 Kanada - Department of Communications Compliance Statement

Dieses digitale Gerät überschreitet nicht die Klasse B-Grenzwerte für Störgeräuschemissionen digitaler Geräte gemäß dem Standard für Interferenz verursachende Geräte mit dem Titel "Digital Apparatus" (ICES-003) des Department of Communications.

Dieses Gerät ist konform mit Abschnitt 15 der FCC-Vorschriften und dem Kanadischen Standard RSS-210. Der Betrieb unterliegt den folgenden Bedingungen:

- Dieses Gerät darf keine schädlichen Störungen verursachen.
- Dieses Gerät muss alle Störungen vertragen, einschließlich Störungen, die unerwünschte Funktionen verursachen können.
- Dieses digitale Gerät der Klasse B ist konform mit der kanadischen Norm ICES-003.
- Der Betrieb im 5150-5250 MHz-Band ist nur in geschlossenen Räumen erlaubt, um schädliche Störungen von zweikanaligen mobilen Satellitensystemen zu vermeiden.
- Der zur Gewährleistung der Konformität mit den EIRP-Grenzwerten maximal zulässige Antennengewinn bei Betrieb im 5250-5350 MHz-Band beträgt für die interne Antenne 4,3 dBi und für die standardmäßig mit dem Gerät gelieferte externe Antenne 5 dBi. Informationen zur Einhaltung des EIRP-Grenzwerts bei den optionalen externen Antennen finden Sie in Tabelle 5.
- Der zur Gewährleistung der Konformität mit den EIRP-Grenzwerten maximal zulässige Antennengewinn bei Betrieb im 5725-5825 MHz-Band beträgt für die interne Antenne 4,3 dBi und für die standardmäßig mit dem Gerät gelieferte externe Antenne 5 dBi. Informationen zur Einhaltung des EIRP-Grenzwerts bei den optionalen externen Antennen finden Sie in Tabelle 5.
- Beachten Sie, dass leistungsstarke Radaranlagen als Primärnutzer (d.h. mit Priorität) zugewiesen werden und dass diese Radaranlagen Störungen im 5250-5350 MHz- und 5470-5725 MHz-Band von LE-LAN-Geräten verursachen können.

Dieses Gerät erfüllt die folgenden Konformitätsstandards:

Kanadische Konformitätsstandards

Sicherheit

- C22.2 Nr.60950-1-03
- UL 2043 Plenum Rated als Teil von UL 60950-1. Geeignet für die Verwendung in Luftraum-Umgebung gemäß Abschnitten 2-128, 12-010(3) und 12-100 des Canadian Electrical Code, Abschnitt 1, C22.1

EMV

- ICES-003, Klasse B

Funk-Transceiver

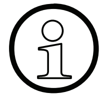
- IC: 4702A-APXXXX
- RSS-210 (2,4 GHz und 5 GHz)

Sonstige

- IEEE 802.11a (5 Ghz)
- IEEE 802.11b/g (2,4 GHz)
- IEEE 802.3af (PoE)

2.1.2.1 Optionale externe Antennen von Drittanbietern

Der Standalone Access Point AP2640 kann auch mit optionalen Drittanbieter-Antennen betrieben werden, sofern diese zertifiziert sind. Möglicherweise ist jedoch eine Genehmigung durch die nationale Regulierungsbehörde erforderlich, um die Übereinstimmung mit lokalen Gesetzen und Vorschriften zu gewährleisten. Die folgenden optionalen Antennen wurden für die Verwendung mit dem Modell mit externer Antenne getestet und genehmigt.



- Bei Verwendung einer genehmigten externen Antenne eines Drittanbieters (keine Standardantenne) muss die Leistung entsprechend den nachfolgenden Tabellen eingestellt werden.
- Das Gerät muss professionell installiert werden. Für eine professionelle Installation bestehen folgende Voraussetzungen:

Vermarktung der Ausrüstung

- Das Gerät darf nicht über den Einzelhandel oder Bestellhandel an die allgemeine Öffentlichkeit verkauft werden. Es muss an Händler verkauft werden.

Professionelle Installation:

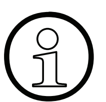
- Die Installation muss überwacht werden.
- Die Installation muss durch lizenziertes Fachpersonal erfolgen (Ausrüstung wird an Händler verkauft, die professionelles Installationspersonal beauftragen)
- Die Installation erfordert eine spezielle Schulung (spezielle Anleitung für Programmierung und Antennen- und Kabelinstallation)

Verwendung

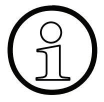
- Die Ausrüstung ist nicht zur Verwendung durch die allgemeine Öffentlichkeit vorgesehen, sondern dient zum industriellen/kommerziellen Einsatz.

#	Modell*	Verwendung	Form	Gewinn (dBi)	Frequenz (MHz)	Koaxkabel Länge/Typ	Anschluss-typ
			Cushcraft				
#1	SR240513 5Dxxxxxx	Indoor	Gerichtet	5	2400-2500	1 Meter / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
#2	S24493DS xxxxxx	Indoor	Omni, 2 Eingänge	3	2400-2500 4900-5990	1 Meter / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 2 St.
#3	SL24513P xxxxxx	Indoor	Omni	3	2400-2500 5150-5350	1 Meter / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
#4	S24497Px xxxxx	Indoor	Gerichtet	7	2400-2500 4900-5990	1 Meter / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA
			Hyperlink Tech				
#5	HG2458C Uxxx	Indoor	Omni	3	2300-2600 4900-6000	30 cm / 20AWG Coleman Cable 921021	N-Buchse
			Maxrad				
#6	MDO2400 5PTxxxxxx	Indoor	Omni, 2 Eingänge	5,2	2400-2485	1 Meter / 19AWG CMP(ETL) C(ETL) 9700851	RPSMA, 2 St.

Tabelle 4   Liste der durch IC (Industry Canada) genehmigten Antennen



Die Qualifizierungstests und -ergebnisse basieren auf den oben beschriebenen Antennen, Kabeltypen/-längen und Anschlusstypen. Weitere Kabellängen und Anschlusstypen sind verfügbar und werden durch den Suffixteil der Teilenummern angegeben (z.B. SR2405135Dxxxxxx, wobei das Suffix xxxxxx für die Kabellänge und/oder den Anschlusstyp steht). Bei den Tests wurde als Antennen-Feedline die minimale Kabellänge verwendet. Es dürfen längere Kabel verwendet werden, deren Verlust größer oder gleich den bei den Tests verwendeten Kabeln ist. Die Einstellungen für die maximale Leistung müssen gemäß diesen Tabellen erfolgen.



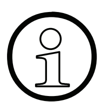
Wenn eine der folgenden Antennen verwendet wird, müssen Sie einen Betriebskanal (auf den Registerkarten **Erweitert 802.11b/g** und **Erweitert 802.11a**) und die entsprechende zulässige max. Leistung aus den in Tabelle 5 aufgelisteten Werten auswählen. Wählen Sie KEINEN HÖHEREN Leistungswert als den in Tabelle 5 aufgelisteten aus.

Antenne			**Antenne #1 Cushcraft SR2405135D xxxxxx**	**Antenne #2 Cushcraft S24493DSxx xxxx**	**Antenne #3 Cushcraft SL24513Pxx xxxx**	**Antenne #4 Cushcraft S24497Pxx xxxx**	**Antenne #5 Hyperlink Tech HG2458CUxxx**	**Antenne #6 Maxrad MDO24005P Txxxxxx**
	Frequenz (MHz)	Ka.-Nr.	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)
11b	2412	1	16	18	17	16	17	17
	2417	2	17	17	17	16	17	17
	2422	3	18	18	18	18	18	18
	2427	4	18	18	18	18	18	18
	2432	5	18	18	18	18	18	18
	2437	6	18	18	18	18	18	18
	2442	7	18	18	18	18	18	18
	2447	8	18	18	18	18	18	18
	2452	9	18	18	18	18	18	18
	2457	10	18	18	18	18	18	18
	2462	11	18	18	18	18	18	18

Tabelle 5 Kanal-Leistungsdaten für IC-Antennen

Antenne			Antenne #1 Cushcraft SR2405135D xxxxxx	Antenne #2 Cushcraft S24493DSxx xxxx	Antenne #3 Cushcraft SL24513Pxx xxxx	Antenne #4 Cushcraft S24497Pxx xxxx	Antenne #5 Hyperlink Tech HG2458CUxxx	Antenne #6 Maxrad MDO24005P Txxxxxx
	Frequenz (MHz)	Ka.-Nr.	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)
11g	2412	1	10	13	13	10	12	13
	2417	2	14	15	15	14	15	14
	2422	3	15	16	16	15	16	16
	2427	4	16	18	18	16	17	17
	2432	5	16	18	18	17	18	18
	2437	6	16	18	18	17	18	18
	2442	7	18	18	18	18	18	18
	2447	8	18	18	18	18	18	18
	2452	9	18	18	18	18	18	18
	2457	10	17	17	17	17	17	18
	2462	11	14	14	14	14	14	14
11a	5180	36	n. unterst.	17	17	17	17	n. unterst.
	5200	40	n. unterst.	17	17	17	17	n. unterst.
	5220	44	n. unterst.	17	17	17	17	n. unterst.
	5240	48	n. unterst.	17	17	17	17	n. unterst.
	5260	52	n. unterst.	18	18	18	18	n. unterst.
	5280	56	n. unterst.	18	18	18	18	n. unterst.
	5300	60	n. unterst.	18	18	18	18	n. unterst.
	5320	64	n. unterst.	18	18	18	18	n. unterst.
	5745	149	n. unterst.	15	n. unterst.	15	15	n. unterst.
	5765	153	n. unterst.	15	n. unterst.	15	15	n. unterst.
	5785	157	n. unterst.	14	n. unterst.	14	14	n. unterst.
	5805	161	n. unterst.	14	n. unterst.	14	14	n. unterst.
	5825	165	n. unterst.	14	n. unterst.	14	14	n. unterst.

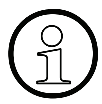
Tabelle 5   Kanal-Leistungsdaten für IC-Antennen



Kanäle mit der Angabe "n. unterst." werden von der Antenne nicht unterstützt und dürfen auf den Registerkarten **Erweitert 802.11b/g** und **Erweitert 802.11a** nicht ausgewählt werden.



Wählen Sie bei der Antenne #3 (Cushcraft SL24513Pxxxxxx) nicht die Kanalauswahl-Option **Auto** (auf der Registerkarte **Erweitert 802.11a**) für das 11a-Funkmodul aus. Wählen Sie stattdessen nur einen Kanal aus der Liste der unterstützten Kanäle in Tabelle 2 aus.
Der Betrieb eines NICHT unterstützten Kanals ist gesetzwidrig.



Wenn Sie für die Kanalauswahl die Option **Auto** auswählen (auf den Registerkarten **Erweitert 802.11b/g** und **Erweitert 802.11a**), müssen Sie auch die in Tabelle 6 aufgelisteten Leistungswerte auswählen. Wählen Sie KEINEN HÖHEREN Leistungswert als den in Tabelle 6 aufgelisteten aus.

Antenne	11a (dBm)	11b/g (dBm)
#1	n. unterst.	10
#2	14	13
#3	17	13
#4	14	10
#5	14	12
#6	n. unterst.	13

Tabelle 6 Automatische Kanalwahl

RF-Sicherheitsabstand

Die für diesen Sender verwendeten Antennen müssen so installiert werden, dass mindestens ein Sicherheitsabstand von 20 cm zu Personen eingehalten wird, und dürfen nicht zusammen mit einer anderen Antenne oder einem anderen Sender installiert oder betrieben werden.

2.1.3 Europäische Union

Der Standalone Access Point AP2630 und AP2640 (AP26XX-Serie) ist für den Einsatz in der Europäischen Union und anderen Ländern mit ähnlichen gesetzlichen Bestimmungen vorgesehen, wobei der Endbenutzer oder Einrichter den Standalone Access Point für den Betrieb konfigurieren darf, indem er einen für das spezielle Land vorgesehenen Ländercode eingibt. Während der Konfiguration wird der Benutzer von der Software aufgefordert, einen Ländercode auszuwählen. Nach Auswahl des Ländercodes wird der Standalone Access Point mit den korrekten Frequenzen und Ausgangsleistungswerten für diesen Ländercode eingerichtet.

Der Standalone Access Point ist für die Verwendung in geschlossenen Räumen (Indoor) vorgesehen und muss in entsprechenden Räumlichkeiten installiert werden, wobei die Verwendung im Freien (Outdoor) unter Umständen zulässig sein kann, wenn bestimmte Frequenzen eingehalten werden und/oder eine entsprechende Betriebslizenz vorliegt. Verwenden Sie das Installationsprogramm, um die korrekte Einrichtung in Übereinstimmung mit den entsprechenden europäischen Bestimmungen bezüglich des genutzten Funkspektrums zu gewährleisten. Wenden Sie sich an die lokalen Behörden, um Informationen zu Vorgehensweisen und gesetzlichen Bestimmungen zu erhalten. Weitere Einzelheiten zu rechtlich zulässigen Kombinationen von Frequenzen, Ausgangspegeln und Antennen erfahren Sie bei Ihrem Siemens-Ansprechpartner.

Erklärung der Konformität mit der RTTE-Richtlinie der Europäischen Union 1999/5/EG

Das folgende Zeichen gewährleistet die Konformität mit den grundlegenden Anforderungen der RTTE-Richtlinie der Europäischen Union (1999/5/EG).





Der Standalone Access Point entspricht den Konformitätsbestimmungen der EG-Richtlinie 2002/95/EG, durch die die Verwendung von bestimmten gefährlichen Stoffen (RoHS) in Elektro- und Elektronikgeräten beschränkt wird.

2.1.3.1 Konformitätserklärung in den Sprachen der Europäischen Union

English	Hereby, Siemens, declares that this Radio LAN device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Finnish	Valmistaja Siemens vakuuttaa täten että Radio LAN device tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Dutch	Hierbij verklaart Siemens dat het toestel Radio LAN device in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. Bij deze verklaart Siemens dat deze Radio LAN device voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
French	Par la présente Siemens déclare que l'appareil Radio LAN device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. Par la présente, Siemens déclare que ce Radio LAN device est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables.
Swedish	Härmed intygar Siemens att denna Radio LAN device står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
Danish	Undertegnede Siemens erklærer herved, at følgende udstyr Radio LAN device overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
German	Hiermit erklärt Siemens die Übereinstimmung des "WLAN Wireless Controller bzw. Access Points" mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG.
Greek	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Siemens ΔΗΛΩΝΕΙ ΟΤΙ Radio LAN device ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Icelandic	Siemens lysir her med yfir að thessi bunadur, Radio LAN device, uppfyllir allar grunnkrofur, sem gerdar eru i R&TTE tilskipun ESB nr 1999/5/EC.
Italian	Con la presente Siemens dichiara che questo Radio LAN device è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Spanish	Por medio de la presente Siemens declara que el Radio LAN device cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

Portuguese	Siemens declara que este Radio LAN device está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Malti	Hawnhekk, Siemens, jiddikjara li dan Radio LAN device jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.

Anforderungen neuer Mitgliedstaaten bezüglich Konformitätserklärung

Estonian	Käesolevaga kinnitab Siemens seadme Radio LAN device vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
Hungary	Alulírott, Siemens nyilatkozom, hogy a Radio LAN device megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Slovak	Siemens týmto vyhlasuje, že Radio LAN device spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Czech	Siemens tímto prohlašuje, že tento Radio LAN device je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES."
Slovenian	Šiuo Siemens deklaruoja, kad šis Radio LAN device atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Latvian	Ar šo Siemens deklarē, ka Radio LAN device atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem
Lithuanian	Siemens deklaruoja, kad Radio LAN device atitinka 1999/5/EC Direktyvos esminius reikalavimus ir kitas nuostatas".
Polish	Niniejszym, Siemens, deklaruję, że Radio LAN device spełnia wymagania zasadnicze oraz stosowne postanowienia zawarte Dyrektywie 1999/5/EC.

Europäische Konformitätsstandards

Sicherheit

- Niederspannungsrichtlinie 73/23/EWG
- EN 60950-1

EMV (Emissionen / Verträglichkeit)

- EMV-Direktive 89/336/EWG
- EN 55011/CISPR 11, Klasse B, Gruppe 1 ISM
- EN 55022/CISPR 22, Klasse B
- EN 55024:1998 Klasse A, beinhaltet IEC/EN 61000-4-2,3,4,5,6,11
- EN 61000-3-2 und -3-3 (Harmonics & Flicker)
- EN 60601-1-2 (Elektromagnetische Verträglichkeit für Medizinprodukte)
- EN 50385 (EMF)
- EN/ETSI 301 489-1 & -17

Funk-Transceiver

- RTTE-Richtlinie 1999/5/EG
- ETSI/EN 300 328-2 2003-04 (2,4 GHz)
- ETSI/EN 301 893-1 2002-07 (5 GHz)

Sonstige

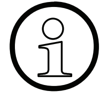
- IEEE 802.11a (5 Ghz)
- IEEE 802.11b/g (2,4 GHz)
- IEEE 802.3af (PoE)

RoHS (Restriction of the use of certain hazardous substances in electrical and electronic equipment, dt.: Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten)

- EG-Richtlinie 2002/95/EG

2.1.3.2 Optionale externe Antennen von Drittanbietern

Der Standalone Access Point AP2640 kann auch mit optionalen Drittanbieter-Antennen betrieben werden, sofern diese zertifiziert sind. Möglicherweise ist jedoch eine Genehmigung durch die nationale Regulierungsbehörde erforderlich, um die Übereinstimmung mit lokalen Gesetzen und Vorschriften zu gewährleisten. Die folgenden optionalen Antennen wurden für die Verwendung mit dem Modell mit externer Antenne getestet und genehmigt.



- Bei Verwendung einer genehmigten externen Antenne eines Drittanbieters (keine Standardantenne) muss die Leistung entsprechend den nachfolgenden Tabellen eingestellt werden.
- Das Gerät muss professionell installiert werden. Für eine professionelle Installation bestehen folgende Voraussetzungen:

Vermarktung der Ausrüstung

- Das Gerät darf nicht über den Einzelhandel oder Bestellhandel an die allgemeine Öffentlichkeit verkauft werden. Es muss an Händler verkauft werden.

Professionelle Installation

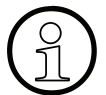
- Die Installation muss überwacht werden.
- Die Installation muss durch lizenziertes Fachpersonal erfolgen (Ausrüstung wird an Händler verkauft, die professionelles Installationspersonal beauftragen)
- Die Installation erfordert eine spezielle Schulung (spezielle Anleitung für Programmierung und Antennen- und Kabelinstallation)

Verwendung

- Die Ausrüstung ist nicht zur Verwendung durch die allgemeine Öffentlichkeit vorgesehen, sondern dient zum industriellen/kommerziellen Einsatz.

#	Modell	Einsatzort	Typ	Gewinn (dBi)	Frequenz (MHz)
Huber+Suhner					
#1	SOA 2454/360/7/20/DF	Outdoor-fähig	Omni	6 8	2400-2500 4900-5875
#2	SPA 2456/75/9/0/DF	Outdoor-fähig	Planar 1 oder 2 Eingänge	9	2400-2500 5150-5875
#3	SPA 2400/80/9/0/DS	Outdoor-fähig	Planar 2 Eingänge	8,5	2300-2500
#4	SWA 0859/360/4/10/V	Outdoor-fähig	Omni	7	2400-5875
#5	SOA 2400/360/4/0/DS	Outdoor-fähig	Omni	3,5	2400-2500
#6	SPA 2400/40/14/0/DS	Outdoor-fähig	Planar 2 Eingänge	13,5	2400-2500
#7	SWA 2459/360/4/45/V	Outdoor-fähig	Omni	>4	2400-5875

Tabelle 7 Liste der genehmigten Antennen für Europa



Wenn eine der folgenden Antennen verwendet wird, müssen Sie einen Betriebskanal (auf den Registerkarten **Erweitert 802.11b/g** und **Erweitert 802.11a**) und die entsprechende zulässige max. Leistung aus den in Tabelle 8 aufgelisteten Werten auswählen. Wählen Sie KEINEN HÖHEREN Leistungswert als den in Tabelle 8 aufgelisteten aus.

Antenne			Antenne #1 Huber +Suhner SOA 2454/ 360/7/20/ DF	Antenne #2 Huber +Suhner SPA 2456/ 75/9/0/DF	Antenne #3 Huber +Suhner SPA 2400/80/ 9/0/DS	Antenne #4 Huber +Suhner SWA 0859/ 360/4/10/V	Antenne #5 Huber +Suhner SOA 2400/ 360/4/0/DS	Antenne #6 Huber +Suhner SPA 2400/ 40/14/0/DS	Antenne #7 Huber +Suhner SWA 2459/ 360/4/45/V
	Frequenz (MHz)	Ka.-Nr.	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)
11b	2412	1	15	14	14	15	15	9	15
	2417	2	15	14	14	15	15	9	15
	2422	3	15	14	14	15	15	9	15
	2427	4	15	14	14	15	15	9	15
	2432	5	15	14	14	15	15	9	15
	2437	6	15	14	14	15	15	9	15
	2442	7	15	14	14	15	15	9	15
	2447	8	15	14	14	15	15	9	15
	2452	9	15	14	14	15	15	9	15
	2457	10	15	14	14	15	15	9	15
	2462	11	15	14	14	15	15	9	15
	2467	12	15	14	14	15	15	9	15
	2472	13	15	14	15	15	15	10	15

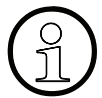
Tabelle 8 Kanal-Leistungsdaten für ETSI-Antennen

Antenne			Antenne #1 Huber +Suhner SOA 2454/ 360/7/20/ DF	Antenne #2 Huber +Suhner SPA 2456/ 75/9/0/DF	Antenne #3 Huber +Suhner SPA 2400/80/ 9/0/DS	Antenne #4 Huber +Suhner SWA 0859/ 360/4/10/V	Antenne #5 Huber +Suhner SOA 2400/ 360/4/0/DS	Antenne #6 Huber +Suhner SPA 2400/ 40/14/0/DS	Antenne #7 Huber +Suhner SWA 2459/ 360/4/45/V
	Frequenz (MHz)	Ka.-Nr.	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)
11g	2412	1	15	13	14	15	15	9	15
	2417	2	15	13	14	15	15	9	15
	2422	3	15	13	14	15	15	9	15
	2427	4	15	13	14	15	15	9	15
	2432	5	15	13	14	15	15	9	15
	2437	6	15	13	14	15	15	9	15
	2442	7	15	14	14	15	15	10	15
	2447	8	15	14	14	15	15	10	15
	2452	9	15	14	14	15	15	10	15
	2457	10	15	14	14	15	15	10	15
	2462	11	15	14	14	15	15	10	15
	2467	12	15	14	14	15	15	10	15
	2472	13	15	13	13	15	15	9	15

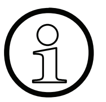
Tabelle 8 Kanal-Leistungsdaten für ETSI-Antennen

Antenne			Antenne #1 Huber +Suhner SOA 2454/ 360/7/20/ DF	Antenne #2 Huber +Suhner SPA 2456/ 75/9/0/DF	Antenne #3 Huber +Suhner SPA 2400/80/ 9/0/DS	Antenne #4 Huber +Suhner SWA 0859/ 360/4/10/V	Antenne #5 Huber +Suhner SOA 2400/ 360/4/0/DS	Antenne #6 Huber +Suhner SPA 2400/ 40/14/0/DS	Antenne #7 Huber +Suhner SWA 2459/ 360/4/45/V
	Frequenz (MHz)	Ka.-Nr.	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)	Leistungs-grenze (dBm)
11a	5180	36	16	16	n. unterst.	16	n. unterst.	n. unterst.	16
	5200	40	16	16	n. unterst.	16	n. unterst.	n. unterst.	16
	5200	44	16	16	n. unterst.	16	n. unterst.	n. unterst.	16
	5240	48	16	16	n. unterst.	16	n. unterst.	n. unterst.	16
	5260	52	16	16	n. unterst.	16	n. unterst.	n. unterst.	16
	5280	56	16	16	n. unterst.	16	n. unterst.	n. unterst.	16
	5300	60	16	16	n. unterst.	16	n. unterst.	n. unterst.	16
	5320	64	16	16	n. unterst.	16	n. unterst.	n. unterst.	16
	5500	100	20	19	n. unterst.	20	n. unterst.	n. unterst.	20
	5520	104	20	19	n. unterst.	20	n. unterst.	n. unterst.	20
	5540	108	20	19	n. unterst.	20	n. unterst.	n. unterst.	20
	5560	112	20	19	n. unterst.	20	n. unterst.	n. unterst.	20
	5580	116	20	19	n. unterst.	20	n. unterst.	n. unterst.	20
	5600	120	20	19	n. unterst.	20	n. unterst.	n. unterst.	20
	5620	124	20	19	n. unterst.	20	n. unterst.	n. unterst.	20
	5640	128	20	19	n. unterst.	20	n. unterst.	n. unterst.	20
	5660	132	20	19	n. unterst.	20	n. unterst.	n. unterst.	20
	5680	136	20	19	n. unterst.	20	n. unterst.	n. unterst.	20
	5700	140	20	19	n. unterst.	20	n. unterst.	n. unterst.	20

Tabelle 8 Kanal-Leistungsdaten für ETSI-Antennen



Kanäle mit der Angabe "n. unterst." werden von der Antenne nicht unterstützt und dürfen auf den Registerkarten **Erweitert 802.11b/g** und **Erweitert 802.11a** nicht ausgewählt werden.



Wenn Sie für die Kanalauswahl die Option **Auto** auswählen (auf den Registerkarten **Erweitert 802.11b/g** und **Erweitert 802.11a**), müssen Sie auch die in Tabelle 9 aufgelisteten Leistungswerte auswählen. Wählen Sie KEINEN HÖHEREN Leistungswert als den in Tabelle 9 aufgelisteten aus.

Antenne	11a (dBm)	11b/g (dBm)
#1	16	15
#2	16	13
#3	n. unterst.	13
#4	16	15
#5	n. unterst.	15
#6	n. unterst.	9
#7	16	15

Tabelle 9 Automatische Kanalwahl

RF-Sicherheitsabstand

Die für diesen Sender verwendeten Antennen müssen so installiert werden, dass mindestens ein Sicherheitsabstand von 20 cm zu Personen eingehalten wird, und dürfen nicht zusammen mit einer anderen Antenne oder einem anderen Sender installiert oder betrieben werden.

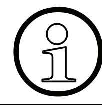
2.1.3.3 Bedingungen für den Betrieb in der Europäischen Union

Die Standalone Access Points AP2630 und AP2640 (AP26XX-Serie) mit interner und externer Antenne sind für den Indoor-Betrieb vorgesehen. In einigen EU-Ländern ist der Outdoor-Betrieb unter Einschränkungen zulässig, die in diesem Abschnitt beschrieben werden. Der Endbenutzer ist dafür verantwortlich, den Betrieb in Übereinstimmung mit diesen Bestimmungen bezüglich Frequenzen und Sendeleistung zu gewährleisten. Der Standalone Access Point darf erst betrieben werden, nachdem er für den geographischen Standort des Kunden korrekt konfiguriert wurde.



Der Benutzer oder Einrichter ist dafür verantwortlich, dass der Standalone Access Point gemäß den Vorschriften bezüglich zulässiger Frequenzkanäle, Einschränkung des Indoor-/Outdoor-Betriebs, erforderlichen Lizenzen und zulässiger Sendeleistung des jeweiligen Landes betrieben wird. Im Lieferumfang des Standalone Access Point ist ein Konfigurationsprogramm enthalten, mit dem der Endbenutzer die Konfiguration überprüfen und erforderliche Konfigurationsänderungen vornehmen kann, um den ordnungsgemäßen Betrieb gemäß den Konformitätsbestimmungen der Europäischen RTTE-Richtlinie 1999/5/EG bezüglich des genutzten Funkspektrums zu gewährleisten.

Die Standalone Access Points mit interner und externer Antenne sind in allen Ländern der Europäischen Union ausschließlich für den Betrieb in geschlossenen Räumen (Indoor-Betrieb) vorgesehen. In einigen Ländern gelten Einschränkungen bezüglich der Betriebskanäle. Diese Einschränkungen werden in diesem Abschnitt beschrieben.



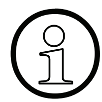
Bitte beachten Sie die Hinweise in dieser Bedienungsanleitung, um den Standalone Access Point korrekt zu konfigurieren.

- Beim Standalone Access Point muss der Endbenutzer oder Einrichter über eine gültige Lizenz verfügen, um den Standalone Access Point betreiben zu können. Die Lizenz enthält die Region, und die Region gibt die Ländercodes an, die die korrekte Konfiguration in Übereinstimmung mit den europäischen und nationalen Bestimmungen bezüglich des genutzten Funkspektrums ermöglichen.
- Es gibt eine Standardgruppe mit Einstellungen in jedem Standalone Access Point. Diese Einstellungen können geändert werden. Der Benutzer oder Einrichter ist dafür verantwortlich, dass jeder Standalone Access Point korrekt konfiguriert ist.
- Die Software in dem Standalone Access Point schränkt die zulässigen Kanäle und die erlaubte Ausgangsleistung automatisch gemäß dem ausgewählten Ländercode ein. Die Auswahl eines nicht korrekten Betriebslandes oder die unkorrekte Angabe der verwendeten Antenne kann dazu führen, dass der Betrieb des Geräts gesetzwidrig ist und dass es zu schädlichen Störungen anderer Anlagen kommt.

• Dieses Gerät verwendet eine Radarortungsfunktion, die für den Betrieb im 5-GHz-Band in der Europäischen Union benötigt wird. Diese Funktion wird automatisch aktiviert, wenn das Betriebsland korrekt als ein Land der Europäischen Union konfiguriert ist. Der Betrieb von Radaranlagen in der Nähe kann dazu führen, dass der Betrieb dieses Geräts vorübergehend unterbrochen wird. Die Radarortungsfunktion nimmt den Betrieb automatisch auf einem Kanal ohne Radarbetrieb wieder auf.
• Der 5-GHz-Turbomodus kann auf dem Standalone Access Point nicht aktiviert werden.
• Die in diesem Bedienerhandbuch beschriebene Einstellung **Auto** für die Kanalauswahl im 5-GHz-Band muss immer aktiviert sein, um sicherzustellen, dass die automatische 5-GHz-Kanalauswahl den europäischen Bestimmungen entspricht.
• Das 5150-5350 MHz-Band, Kanäle 36, 40, 44, 48, 52, 56, 60 oder 64, ist nur für den Indoor-Einsatz zugelassen.
• Der Standalone Access Point mit externer Antenne darf nur mit von Siemens zertifizierten Antennen betrieben werden.
• Das 2,4-GHz-Band, Kanäle 1 - 13, ist für den Indoor- und Outdoor-Einsatz zugelassen, es können jedoch einige Einschränkungen bezüglich der Kanäle bestehen.
• In Italien muss der Endbenutzer für den Outdoor-Betrieb eine Lizenz von der zuständigen nationalen Behörde beantragen.
• In Belgien ist der Outdoor-Betrieb nur im 2,46 - 2,4835 GHz-Band auf Kanal 13 zulässig.
• In Frankreich ist der Outdoor-Betrieb nur im 2,4 - 2,454 GHz-Band auf den Kanälen 1 - 7 zulässig.

2.1.4 Zertifizierungen anderer Länder

Die Standalone Access Points AP2630 und AP2640 (AP26XX-Serie) wurden für die Verwendung in den Ländern zertifiziert, die in der unten stehenden Tabelle aufgelistet sind. Bei der Konfiguration des Standalone Access Point wird der Benutzer aufgefordert, einen Ländercode auszuwählen. Nach Auswahl des korrekten Ländercodes wird der Standalone Access Point mit den korrekten Frequenzen und Ausgangsleistungswerten für diesen Ländercode eingerichtet.



Der Endbenutzer ist dafür verantwortlich, den korrekten Ländercode für das Land einzugeben, in dem das Gerät betrieben wird, da sonst das Risiko besteht, dass lokale Gesetze und Vorschriften missachtet werden.

Optionale externe Antennen von Drittanbietern

Der Standalone Access Point AP2640 kann auch mit optionalen Drittanbieter-Antennen betrieben werden, sofern diese zertifiziert sind. Möglicherweise ist jedoch eine Genehmigung durch die nationale Regulierungsbehörde erforderlich, um die Übereinstimmung mit lokalen Gesetzen und Vorschriften zu gewährleisten.

Weitere länderspezifische Konformitätsstandards, Genehmigungen und Erklärungen

Australien und Neuseeland

- AS/NZS 4288 (Funk gemäß EU-Standards)
- AS/NZS 60950.1 (Sicherheit)
- AS/NZS 3548 (Emissionen gemäß EU-Standards - ACMA)
- IEEE 802.11a/b/g
- IEEE 802.3af (PoE)
- EN 300 328-2:2003-04 (2,4 GHz)
- EN 301 893-1:2003-08 (5 GHz)
- EN 301 489-17:2002-08 (RLAN)

2.2 Liste der länderspezifischen Unterstützung

Spektrum	**11b/g-Band 1 2,4-2,472/ 2,4835 GHz**	**11a-Band 1 5,15-5,25 GHz**	**11a-Band 2 5,25-5,35 GHz**	**11a-Band 3 5,47-5,725 GHz**	**11a-Band 4 5,725-5,825/ 5,850 GHz**
Kanal-Nr.	**1-11/13**	**36, 40, 44, 48**	**52, 56, 60, 64**	**100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140**	**149, 153, 157, 161 (165)**
Argentinien	11b & g 11 Kanäle	Nicht unterstützt	4 Kanäle	Nicht unterstützt	4 Kanäle
Australien	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	Nicht unterstützt	4 Kanäle
Belgien	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Bosnien-Herzegowina	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Brasilien	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	5 Kanäle
Bulgarien	11b & g 13 Kanäle	4 Kanäle	2 Kanäle	11 Kanäle	Nicht unterstützt
Chile	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	Nicht unterstützt	5 Kanäle
China	11b & g 13 Kanäle	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	5 Kanäle
Deutschland	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Dänemark	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Estland	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Finnland	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Frankreich	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	Nicht unterstützt	Nicht unterstützt

Tabelle 10 Liste der länderspezifischen Unterstützung

Spektrum	**11b/g-Band 1 2,4-2,472/ 2,4835 GHz**	**11a-Band 1 5,15-5,25 GHz**	**11a-Band 2 5,25-5,35 GHz**	**11a-Band 3 5,47-5,725 GHz**	**11a-Band 4 5,725-5,825/ 5,850 GHz**
Kanal-Nr.	**1-11/13**	**36, 40, 44, 48**	**52, 56, 60, 64**	**100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140**	**149, 153, 157, 161 (165)**
Griechenland	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Hongkong	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	Nicht unterstützt	5 Kanäle
Indien	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	Nicht unterstützt	5 Kanäle
Irland	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Island	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Israel	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	Nicht unterstützt	Nicht unterstützt
Italien	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Japan	11b 14 Kanäle 11g 13 Kanäle	4 Kanäle	4 Kanäle	Nicht unterstützt	Nicht unterstützt
Kanada	11b & g 11 Kanäle	4 Kanäle	4 Kanäle	Nicht unterstützt	5 Kanäle
Katar	11b 13 Kanäle	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Kroatien	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Kuwait	11b & g 13 Kanäle	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Lettland	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Litauen	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Luxemburg	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt

Tabelle 10 Liste der länderspezifischen Unterstützung

Spektrum	11b/g-Band 1 2,4-2,472/ 2,4835 GHz	11a-Band 1 5,15-5,25 GHz	11a-Band 2 5,25-5,35 GHz	11a-Band 3 5,47-5,725 GHz	11a-Band 4 5,725-5,825/ 5,850 GHz
Kanal-Nr.	**1-11/13**	**36, 40, 44, 48**	**52, 56, 60, 64**	**100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140**	**149, 153, 157, 161 (165)**
Macau	11b & g 13 Kanäle	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	5 Kanäle
Malaysia	11b & g 13 Kanäle	Nicht unterstützt	4 Kanäle	Nicht unterstützt	5 Kanäle
Malta	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Mexiko	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	Nicht unterstützt	Nicht unterstützt
Neuseeland	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	Nicht unterstützt	5 Kanäle
Niederlande	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Norwegen	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Pakistan	11b 13 Kanäle	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Polen	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Portugal	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Puerto Rico (USA)	11b & g 11 Kanäle	4 Kanäle	4 Kanäle	Nicht unterstützt	5 Kanäle
Rumänien	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Russland	11b 13 Kanäle	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Schweden	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Schweiz & Liechtenstein	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt

Tabelle 10 Liste der länderspezifischen Unterstützung

Spektrum	**11b/g-Band 1 2,4-2,472/ 2,4835 GHz**	**11a-Band 1 5,15-5,25 GHz**	**11a-Band 2 5,25-5,35 GHz**	**11a-Band 3 5,47-5,725 GHz**	**11a-Band 4 5,725-5,825/ 5,850 GHz**
Kanal-Nr.	**1-11/13**	**36, 40, 44, 48**	**52, 56, 60, 64**	**100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140**	**149, 153, 157, 161 (165)**
Serbien & Montenegro	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Singapur	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	Nicht unterstützt	5 Kanäle
Slowakei	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Slowenien	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Spanien	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Südafrika	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Südkorea	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	5 Kanäle	4 Kanäle
Taiwan	11b & g 11 Kanäle	Nicht unterstützt	3 Kanäle	11 Kanäle	4 Kanäle
Thailand	11b & g 13 Kanäle	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Tschechi-sche Rep.	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Türkei	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	Nicht unterstützt	Nicht unterstützt
UK	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Ungarn	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
USA	11b & g 11 Kanäle	4 Kanäle	4 Kanäle	Nicht unterstützt	5 Kanäle
VAE	11b 13 Kanäle	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt

Tabelle 10 Liste der länderspezifischen Unterstützung

Spektrum	11b/g-Band 1 2,4-2,472/ 2,4835 GHz	11a-Band 1 5,15-5,25 GHz	11a-Band 2 5,25-5,35 GHz	11a-Band 3 5,47-5,725 GHz	11a-Band 4 5,725-5,825/ 5,850 GHz
Kanal-Nr.	**1-11/13**	**36, 40, 44, 48**	**52, 56, 60, 64**	**100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140**	**149, 153, 157, 161 (165)**
Venezuela	11b & g 13 Kanäle	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Vietnam	11b & g 13 Kanäle	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt	Nicht unterstützt
Zypern	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt
Österreich	11b & g 13 Kanäle	4 Kanäle	4 Kanäle	11 Kanäle	Nicht unterstützt

Tabelle 10 Liste der länderspezifischen Unterstützung

3 Info zum HiPath Wireless Standalone Access Point

Der Standalone Access Point bietet qualitativ hochwertige und zuverlässige drahtlose Kommunikation. Der auf einer WLAN-Topologie der dritten Generation basierende Standalone Access Point ermöglicht den praktischen Einsatz drahtloser Technologien für kleine und mittlere Unternehmen (SME-Markt). Diese Lösung bietet die Sicherheit und Verwaltbarkeit, die von Unternehmen und Dienstanbietern gleichermaßen gefordert werden.

Der Standalone Access Point ist ein Dual-Band Access Point mit 802.11a+b/g-Funk, der folgende Leistungsmerkmale aufweist:

- Eigenständiger Access Point – Einstiegslösung für den SME-Markt
- End-to-End-Lösung für drahtlose Echtzeit-IP-Kommunikation und HiPath-Integration
- Übergangslose Mobilität
- Beste Sprachqualität seiner Klasse, Multimedia-fähig
- Hohe Sicherheit auf SME-Ebene
- Einfacher Einsatz und Betrieb

3.1 Funktionsweise konventioneller drahtloser LANs

Die drahtlose Kommunikation zwischen zwei oder mehr Computern erfordert, dass jeder Computer mit einer Empfänger/Sender-Vorrichtung – einer WLAN-Netzwerkkarte – ausgestattet ist, die digitale Informationen über gängige Funkfrequenzen übertragen kann. Dies wird als Ad-hoc-Konfiguration bezeichnet. Ein Ad-hoc-Netzwerk ermöglicht die Kommunikation zwischen drahtlosen Geräten. Dies wird als Independent Basic Service Set (IBSS) bezeichnet.

Eine Alternative zur Ad-hoc-Konfiguration ist der Einsatz eines Access Point. Dies kann ein zweckgebundener Hardwarerouter oder ein Computer mit spezieller Software sein. Computer und andere drahtlose Geräte kommunizieren über diesen Access Point miteinander. Der IEEE 802.11-Standard definiert einen Access Point als ein Gerät, das es anderen drahtlosen Geräten ermöglicht, mit einem "Verteilungssystem" zu kommunizieren. Dies wird als Basic Service Set (BSS) oder Infrastruktur-Netzwerk bezeichnet.

Damit drahtlose Geräte mit Computern auf einem drahtgebundenen Netzwerk kommunizieren können, müssen die Access Points mit dem drahtgebundenen Netzwerk verbunden sein und einen Zugang zu den vernetzten Computern bereitstellen. Dies wird als Bridging bezeichnet. Es ist offensichtlich, dass sich bei dieser Anordnung Sicherheits- und Verwaltungsfragen (Skalierbarkeit) stellen.

3.2 Funktionsweise des Standalone Access Point

Der Standalone Access Point ist ein Access Point zu einem drahtlosen LAN. Der Standalone Access Point bietet auch lokale Verarbeitungsfunktionen, zum Beispiel Verschlüsselung. Zusätzlich zum Standalone Access Point wird mit der Lösung auch eine optionale DHCP-Serverkomponente bereitgestellt, die in Enterprise- und Dienstanbieter-Netzwerken zur Standardausstattung gehört. Standalone Access Points sind kostengünstig, einfach zu verwalten und problemlos einzusetzen.

Nachfolgend sind einige Vorteile des Standalone Access Point aufgeführt:

Erhöhte Sicherheit	Die Benutzeroberfläche des Standalone Access Point ist durch Benutzer-IDs und Kennwörter sowie durch formularbasierte Authentifizierung gesichert. Außerdem kann der Benutzer für den Standalone Access Point keine Sicherheit, WEP-Sicherheit oder WPA-PSK-Sicherheit wählen.
Roaming im Subnetz	Der Standalone Access Point bietet die Erstellung und Verwaltung eines Roaming-Clusters und gewährleistet die schnelle Übergabe (Handover) von mobilen Clients innerhalb des Roaming-Clusters.
Fehlerbehebungsfunktionen	Der Standalone Access Point protokolliert System- und Sitzungsaktivitäten und stellt Berichte bereit, die bei der Fehleranalyse helfen können.

Tabelle 11 Vorteile des Standalone Access Point

3.3 Standalone Access Point und Ihr Netzwerk

Vor Verwendung des Standalone Access Point müssen Sie sich mit seinen Komponenten und Sicherheitsfunktionen vertraut machen.

3.3.1 Standalone Access Point-Netzwerkkomponenten

Jedes drahtlose Gerät sendet IP-Pakete gemäß IEEE 802.11-Standard an den Standalone Access Point. Der Standalone Access Point fungiert als Brücke für den Datenverkehr zwischen dem drahtlosen Gerät und dem Netzwerk.

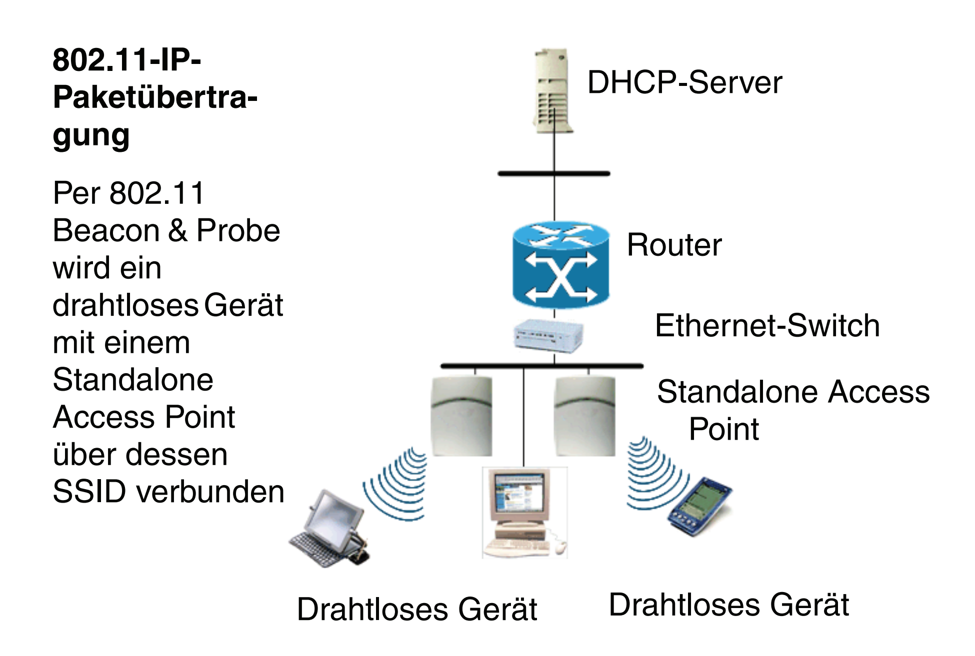


Bild 1 Netzverkehr-Ablaufdiagramm

Weitere Informationen zum DHCP-Server finden Sie in der Dokumentation zu HiPath Wireless.

3.3.2 Info zur Netzwerksicherheit

Der Standalone Access Point stellt Leistungsmerkmale und Funktionen zur Kontrolle des Netzwerkzugangs bereit. Diese basieren auf Standard-Sicherheitspraktiken für drahtlose Netzwerke. Die derzeitigen Sicherheitsverfahren für drahtlose Netzwerke bieten einen gewissen Schutz. Diese Methoden beinhalten ein offenes System, das auf Service Set Identifiers (SSID) beruht.

Der Standalone Access Point unterstützt die folgenden Verschlüsselungsverfahren:

- **Wired Equivalent Privacy (WEP)** – Ein im IEEE 802.11b-Standard definiertes Sicherheitsprotokoll für drahtlose lokale Netzwerke, das statische Schlüsselverwaltung und WEP 40-Bit-, 104-Bit-, und 128-Bit-Verschlüsselung bereitstellt. Das WEP-Protokoll bietet minimale Sicherheit.
- **Wi-Fi Protected Access Version 1 (WPA V.1)** – Ein Sicherheitsprotokoll mit Temporal Key Integrity Protocol (TKIP), das Preshared Master Key-Verwaltung und WEP 128-Bit-Verschlüsselung bereitstellt. Das WPA V.1-Protokoll bietet gute Sicherheit.
- **Wi-Fi Protected Access Version 2 (WPA V.2)** – Ein Sicherheitsprotokoll mit Advanced Encryption Standard (AES), das Preshared Master Key-Verwaltung und AES 128-Bit-Verschlüsselung bereitstellt. Das WPA V.2-Protokoll bietet die beste Sicherheit. Es wird dringend empfohlen, WPA V.2 zu verwenden.

- **Media Access Control-Adresse (MAC)** - Zusätzlich werden MAC-Adressen-Filter zum Sichern des Netzwerks eingesetzt. Die Authentifizierung per MAC-Adresse bietet eine Methode der Benutzer-Zugangssteuerung, bei der die Verbindung zum Access Point basierend auf der MAC-Adresse des Geräts hergestellt wird.

3.3.3 Info zu Quality of Service (QoS)

Der Standalone Access Point stellt mithilfe einer erweiterten Quality of Service (QoS)-Verwaltung einen besseren Netzverkehrsablauf bereit. Folgende Standards sind enthalten:

- **WMM (Wi-Fi Multimedia)** - Per VNS auf dem Standalone Access Point aktiviert. Bei Geräten mit aktiviertem WMM oder 802.1e bietet die Standardkonfiguration Multimedia-Erweiterungen für Audio-, Video- und Sprachanwendungen. WMM und 802.11e verkürzen die Zeit zwischen der Paketübertragung für Datenverkehr mit höherer Priorität.
- **IP ToS (Type of Service) oder DSCP (Diffserve Codepoint)** - Das ToS/DSCP-Feld im IP-Header eines Frames dient zur Angabe der Priorität und der Servicequalität (QoS) für jeden Frame.
- **802.11e** - Wenn diese Option aktiviert ist, akzeptiert der Standalone Access Point 802.11e-Client-Verbindungen und übernimmt die Einstufung und Priorisierung des Downlink-Verkehrs für alle 802.11e-Clients. Die 802.11e-Clients übernehmen auch die Einstufung und Priorisierung des Uplink-Verkehrs.

  Wenn **Prioritätsüberschreibung** aktiviert ist, bestimmt die konfigurierte Benutzerpriorität die Sendewarteschlange und die Benutzerpriorität für die WLAN QoS-Pakete (WMM oder 802.11e) in der Downlink-Richtung. Der Wert für Benutzerpriorität dient auch zum Taggen des Felds VLAN-Priorität für den Uplink-Verkehr, wenn für diesen VNS VLAN-Tagging aktiviert ist.

3.4 Info zu Clustering

Der Standalone Access Point muss in einer Cluster-Konfiguration betrieben werden. Der Zweck des Clusters besteht darin, die Anzahl der darin befindlichen Access Points zu begrenzen und Roaming zu ermöglichen. Secure Inter-Access Point Protocol (SIAPP) dient zum Generieren der Cluster-Informationen in jedem Access Point. Alle Access Points im selben Roaming-Cluster müssen sich auf demselben Subnetz befinden.

3.4.1 Bilden eines Clusters

Ein Cluster wird gebildet, wenn ein Access Point mit einem oder mehreren weiteren Access Points verbunden wird. Ein Cluster wird durch den Clusternamen identifiziert, der auf der SSID basiert. Alle Standalone Access Points in dem Cluster haben einen gemeinsamen Clusternamen. Ein Access Point kann den Zustand Master, Slave oder Register haben. In einem Cluster muss einer der Access Points den Master-Zustand haben. Die Anzahl von

Access Points in dem Cluster kann zu jedem Zeitpunkt maximal 10 betragen, einschließlich der Access Points im Master- und Slave-Zustand, mit aktivierten Funkmodulen. Die Funkmodule sind bei allen Access Points im Register-Zustand deaktiviert.

Der Access Point im Master-Zustand sendet in regelmäßigen Abständen ein Aktualisierungspaket, das die Liste der derzeit in dem Cluster registrierten Access Points enthält. Der erste Access Point in der Liste ist der Master, darauf folgt der erste Slave, der zweite Slave etc.

4 Installieren und Konfigurieren des Standalone Access Point

Vor der Verwendung des Standalone Access Point muss dieser ordnungsgemäß installiert und konfiguriert werden.

4.1 Installieren des Standalone Access Point



Bei der Montage des Standalone Access Point muss auf einen Mindestabstand von 1 Meter zu größeren metallenen Objekten geachtet werden, wenn der Standalone Access Point eine interne oder fest installierte externe Antenne hat.
Wenn die externe Antenne des Standalone Access Point nicht am Access Point selbst angebracht ist, muss die Antenne in einem Mindestabstand von 1 Meter zu größeren metallenen Objekten montiert werden.

So installieren Sie den Standalone Access Point:

1. Nehmen Sie den Standalone Access Point aus dem Verpackungskarton und überprüfen Sie den Inhalt auf Vollständigkeit. Einzelheiten finden Sie in dem mit dem Gerät gelieferten Handbuch *HiPath Wireless Standalone Access Point Getting Started Guide*.
2. Montieren Sie die Wandhalterung mit den 3 vorgesehenen Schrauben in der Nähe des LAN-Ethernet-Kabelsteckers an der Wand.

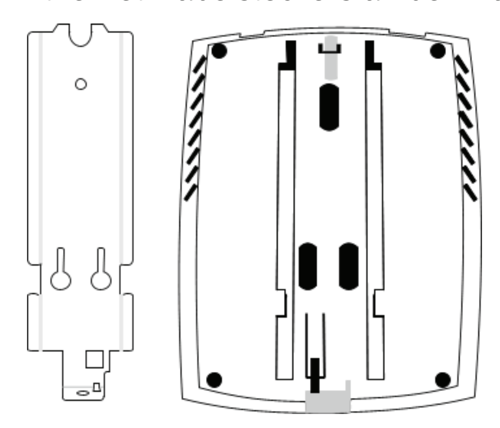


Bild 2 Wandhalterung und Rückansicht des Standalone Access Point

3. Drücken Sie die Rückseite des Standalone Access Point-Gehäuses so auf die Halterung, dass es in die Aussparungen der Halterung passt. Schieben Sie das Gehäuse nach unten, bis die Sicherungsklammer einrastet und es festhält.

Um den Standalone Access Point wieder aus der Halterung zu entfernen, lösen Sie die Sicherungsklammer, indem Sie einen Imbusschlüssel (oder ein ähnliches Werkzeug) in die kleine Öffnung an der Unterseite der Halterung einführen. Schieben Sie dann das Gehäuse des Standalone Access Point nach oben und heben Sie es von der Halterung ab.

4. Führen Sie den Plastik-Spreizniet durch die Öffnung an der Unterseite der Halterung in das Standalone Access Point-Gehäuse ein. Schrauben Sie mit einem Schraubendreher die Plastikschraube in den Niet. Dadurch wird der Niet gespreizt und das Gehäuse mit der Halterung fest verbunden. Um den Standalone Access Point zu entfernen, drehen Sie die Schraube mit einem Schraubendreher wieder heraus.

4.2 Anschlüsse und Stromversorgung für den Standalone Access Point

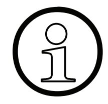


Dieses Gerät darf nicht über Außenverdrahtung an ein LAN-Segment angeschlossen werden.
Stellen Sie sicher, dass alle Kabel korrekt geführt werden, um Zugbelastung zu vermeiden. Sollte das Netzteil Anzeichen von Beschädigung aufweisen, tauschen Sie es sofort aus.

Sie können die LAN-Verbindung und die Stromversorgung des Standalone Access Point auf drei Arten herstellen:

- **Power-over-Ethernet (PoE)** – Wenn Ihr Netzwerk bereits mit PoE eingerichtet ist, schließen Sie das LAN-Ethernet-Kabel an die RJ45-Ethernet-Buchse an der Oberseite des Standalone Access Point an. Für diese Methode können Sie ein Standard-Ethernetkabel verwenden.
- **Power-over-Ethernet: PoE-Injector hinzufügen** – Wenn Ihr Netzwerk nicht für PoE eingerichtet ist, können Sie die Stromversorgung des LAN-Ethernet-Kabels mit einem PoE-Injector bereitstellen. Der PoE-Injector muss 802.3af-kompatibel sein. Der PoE-Injector ist nicht im Lieferumfang des Standalone Access Point enthalten. Wenn Sie einen PoE-Injector verwenden, lesen Sie bezüglich der Anforderungen in der Dokumentation des Herstellers nach.
- **Stromversorgung über AC-Adapter (externes Netzteil)** – Ein AC-Adapter (Netzteil) für den Standalone Access Point wird separat angeboten. Er muss folgende Spezifikationen aufweisen:
  - Eingangsspannung: 120-240 VAC
  - Ausgangsspannung: DC +6V, max. Stromstärke 1,5 A, max. Leistung 10 W

  Bei einer Direktverbindung zum Standalone Access Point muss ein Crossover-Ethernetkabel verwendet werden.



Wenn Sie einen Adapter verwenden, installieren Sie den Standalone Access Point innerhalb einer Entfernung von zwei Metern von einer Wandsteckdose, schließen Sie den Standalone Access Point an den Adapter und dann den Adapter an die Wandsteckdose an.

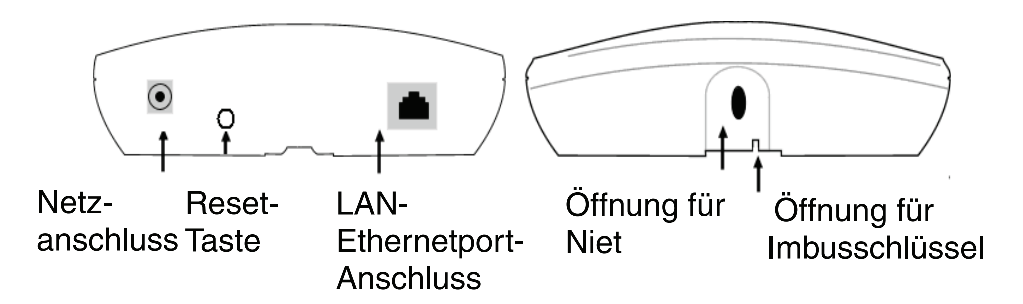


Bild 3 Draufsicht und Unteransicht des Standalone Access Point

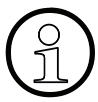
4.3 Erklärung des LED-Status für den Standalone Access Point

Bei der nachfolgenden Beschreibung wird vorausgesetzt, dass die Software einen Zeitgeber und mehrere Phasen verwendet, um LED-"Blinken" auf allen drei LEDs zu simulieren. Beispielsweise bedeutet der LED-Status "Rot", dass die LED die Vollfarbe "Rot" hat, und der LED-Status "Aus/Grün/Aus", dass die LED in der ersten Phase "Aus", in der zweiten Phase "Grün" und in der dritten Phase "Aus" ist.

LED-Status Links	LED-Status Mitte	LED-Status Rechts	Status des Access Point
Aus	Aus	Aus	Ausgeschaltet
Aus	Grün	Aus	Start des Power-On-Self-Tests (POST) (0,5 s)
Aus	Aus	Aus	POST
Aus	Rot	Aus	Fehler während POST
Grün	Aus	Grün	Zufallsverzögerung (Status wird erst nach Vulnerable-Reset gezeigt)
Grün/Aus	Aus/Grün	Grün/Aus	Vulnerable-Time-Intervall (der Standalone Access Point wird auf Standardwerte zurückgesetzt, wenn er während dieses Zustands dreimal hintereinander ausgeschaltet wird). Keine Vulnerable-Time, wenn der Standalone Access Point auf Standardwerte zurückgesetzt wird.

LED-Status Links	LED-Status Mitte	LED-Status Rechts	Status des Access Point
Grün/Aus/ Aus	Aus/Grün/ Aus	Aus/Aus/ Grün	Ansage des Zurücksetzens auf Standardwerte (ersetzt Vulnerable-Time). Dieses Muster wird zweimal wiederholt, um den Bediener zu benachrichtigen, wenn die Standardkonfiguration wiederhergestellt ist.
Aus	Orange (Grün + Rot)/ Grün	Aus	Versuche, IP-Adresse über DHCP zu erhalten
Aus	Aus/Grün	Aus	IP-Adresse erhalten. Versuche, Cluster beizutreten
Grün, wenn 802.11b/g aktiviert Andern-falls Aus	Grün	Grün, wenn 802.11a aktiviert Andernfalls Aus	Mitglied von Cluster, Funk aktiviert durch Benutzereinstellungen

Tabelle 12 Statusdefinitionen für Standalone Access Point-LEDs



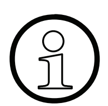
Zufallsverzögerungen treten während normaler Neustarts nicht auf. Zufallsverzögerungen treten nur nach einer Vulnerable-Time-Abschaltung auf.

4.4 Wiederherstellen der werkseitigen Standardeinstellungen

Es gibt drei unterschiedliche Methoden zum Wiederherstellen der werkseitigen Standardeinstellungen für den Standalone Access Point:

- **Vulnerable-Time-Intervall** - Die Startsequenz des Standalone Access Point beinhaltet ein Vulnerable-Time-Intervall. Während des Vulnerable-Time-Intervalls (2 Sekunden) blinken die LEDs in einer bestimmten Reihenfolge, um anzuzeigen, dass der Standalone Access Point sich im Vulnerable-Time-Intervall befindet. Weitere Informationen finden Sie in Tabelle 12 auf Seite 54.

  Wenn Sie den Standalone Access Point starten und während des Vulnerable-Time-Intervalls die Stromversorgung dreimal hintereinander unterbrechen, werden beim nächsten Neustart des Standalone Access Point die werkseitigen Standardwerte einschließlich des Benutzerkennworts und der Standard-IP-Einstellungen wiederhergestellt.



Bei der Wiederherstellung der werkseitigen Standardeinstellungen wird das nicht-flüchtige Protokoll nicht gelöscht.

- **Reset-Taste (Hardware)** - Drücken Sie die **Reset**-Taste auf dem Standalone Access Point, und halten Sie sie für ungefähr fünf Sekunden gedrückt. Der Standalone Access Point wird neu gestartet, und die Standardwerte werden wiederhergestellt.
- **Standardwerte wiederherst. (Benutzeroberfläche)** - Verwenden Sie die Schaltfläche **Standardwerte wiederherst.** im Bildschirm **Extras > Konfiguration**, um die Standardwerte über die Benutzeroberfläche des Standalone Access Point wiederherzustellen. Weitere Informationen finden Sie unter Abschnitt 6.4.3, “Wiederherstellen der werkseitigen Standardeinstellungen”, auf Seite 99.

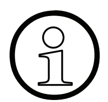
So stellen Sie die werkseitigen Standardeinstellungen mithilfe des Vulnerable-Time-Intervalls wieder her:

1. Starten Sie den Standalone Access Point neu.
2. Schalten Sie den Standalone Access Point während des Vulnerable-Time-Intervalls aus und wieder ein.
3. Wiederholen Sie Schritt 2 zweimal.

   Wenn der Standalone Access Point zum vierten Mal neu gestartet wird, nachdem die Stromversorgung dreimal hintereinander unterbrochen wurde, werden die werkseitigen Standardeinstellungen wiederhergestellt.

5 Erste Schritte mit dem Standalone Access Point

Sie können über einen Webbrowser auf den Standalone Access Point zugreifen.



Die folgenden Abschnitte enthalten Kurzanleitungen zum Installieren und Konfigurieren des HiPath Wireless Standalone Access Point. Weitere Informationen zur Konfiguration und Fehlerbehebung, einschließlich Statusreporte, finden Sie in der *HiPath Wireless Standalone Access Point Getting Started Guide* im Lieferumfang des Standalone Access Point.

5.1 Benutzeroberfläche

Der Standalone Access Point unterstützt zwei Benutzertypen:

- **Administrator** – die Benutzer-ID ist “admin” (Groß-/Kleinschreibung beachten), und das Standardkennwort ist “admin”.
- **Standardbenutzer** – die Benutzer-ID ist “user” (Groß-/Kleinschreibung beachten), und das Standardkennwort ist “user”.

Für jeden Benutzer gibt es zwei Hauptzustände:

- **Anmelden** – dem Benutzer wird ein Formular zur Eingabe seiner ID und seines Kennworts angeboten.
- **Angemeldet** - Der Benutzer hat Zugriff auf ein aus zwei Ebenen bestehendes Menü, das die Navigation durch die gesamte Oberfläche ermöglicht.

Wenn Sie als Administrator angemeldet sind, stellt das Menü der oberen Ebene folgende Optionen bereit:

- **Status** – ermöglicht den Zugriff auf die folgenden Bildschirme: Info, Protokolle, LAN, 802.11b/g, 802.11a, Clients und Cluster.
- **Konfiguration** - Ermöglicht den Zugriff auf die folgenden Bildschirme: **LAN** und **WLAN**. Im Bildschirm **WLAN** stehen eine Registerkarte für die **Basiskonfiguration** und vier erweiterte Registerkarten zur Verfügung: **Filter**, **Erweitert 802.11b/g**, **Erweitert 802.11a** und **QoS**. Zusätzlich gibt es Registerkarten für die Konfiguration jedes einzelnen VNS: **Allgemein**, **RF**, **Sicherheit** und **QoS**.
- **Extras** – ermöglicht den Zugriff auf die folgenden Bildschirme: Kennwörter, Konfiguration, Firmware/Sprache und BootROM.
- **Hilfe** – ermöglicht den Zugriff auf die Online-Hilfe für jeden Bildschirm der Benutzeroberfläche.

- **Abmelden** – meldet den aktuellen Benutzer von der Standalone Access Point-Benutzeroberfläche ab.

Wenn Sie als Standardbenutzer angemeldet sind, stellt das Menü der oberen Ebene folgende Optionen bereit:

- **Status** – ermöglicht den Zugriff auf die folgenden Bildschirme: Info, Protokolle, LAN, 802.11b/g, 802.11a, Clients und Cluster.
- **Hilfe** – ermöglicht den Zugriff auf die Online-Hilfe für jeden Bildschirm der Benutzeroberfläche.
- **Abmelden** – meldet den aktuellen Benutzer von der Standalone Access Point-Benutzeroberfläche ab.

5.2 Anmelden am Standalone Access Point

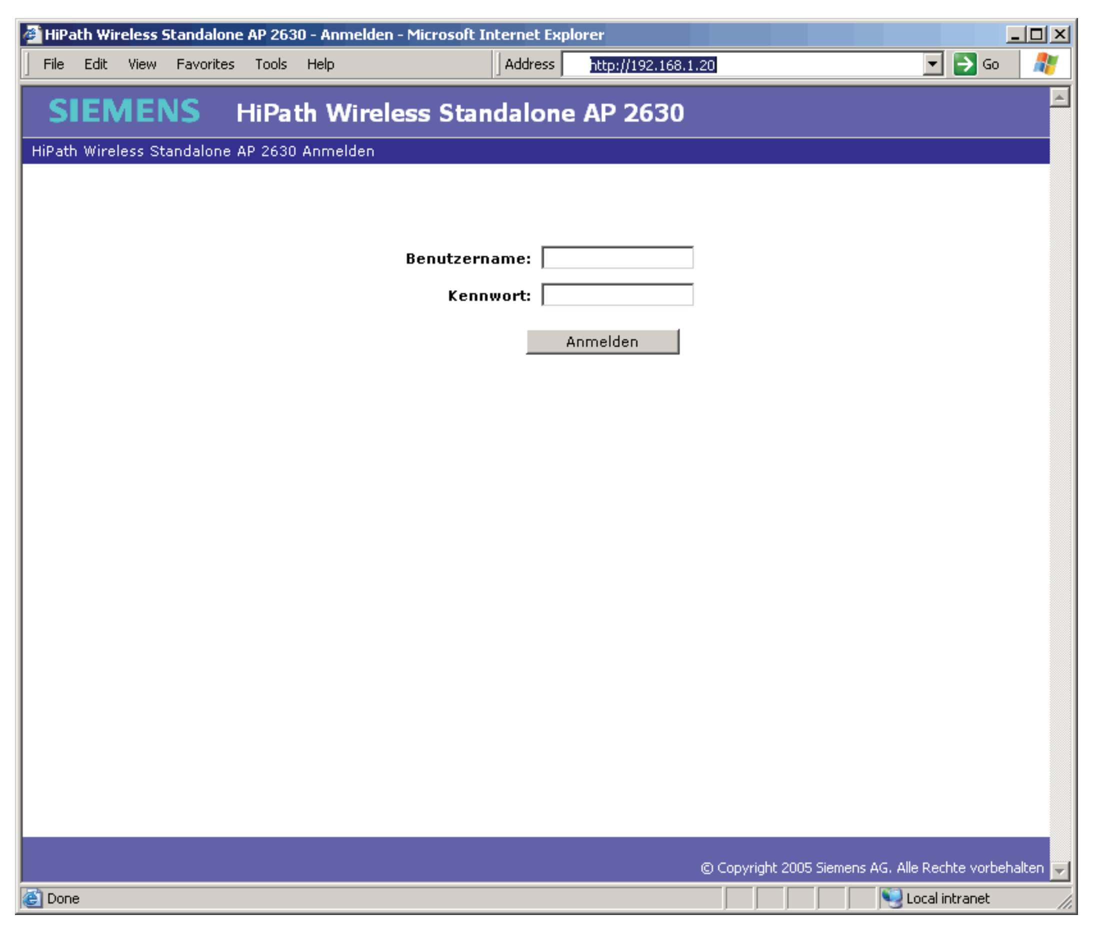
Um auf den Standalone Access Point zugreifen zu können, müssen Sie sich mit einer gültigen Benutzer-ID und dem zugehörigen Kennwort anmelden.

Der Standalone Access Point ist standardmäßig DHCP-aktiviert. Verwenden Sie zum Anmelden die IP-Adresse, die der Ihnen im Netzwerk zugewiesenen DHCP-IP-Adresse entspricht. Wenn der Standalone Access Point keine IP-Adresse über DHCP abrufen kann, verwenden Sie die Standard-IP-Adresse 192.168.1.20.

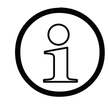
So melden Sie sich bei dem Standalone Access Point an:

1. Geben Sie in einem Webbrowser folgende Adresse ein:

   `http://192.168.1.20`

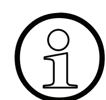


2. Geben Sie in das Feld **Benutzername** die Ihnen zugewiesene eindeutige Benutzer-ID ein.
3. Geben Sie in das Feld **Kennwort** das zu Ihrer Benutzer-ID gehörige Kennwort ein.



Es wird dringend empfohlen, das Kennwort nach der ersten Anmeldung zu ändern.

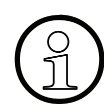
4. Klicken Sie auf **Anmelden**.



Die Websitzung wird nach 900 Sekunden (15 Minuten) ohne Aktivität automatisch beendet.

5.3 Ändern von Kennwörtern

Verwenden Sie den Bildschirm **Kennwörter**, um Kennwörter zu ändern.

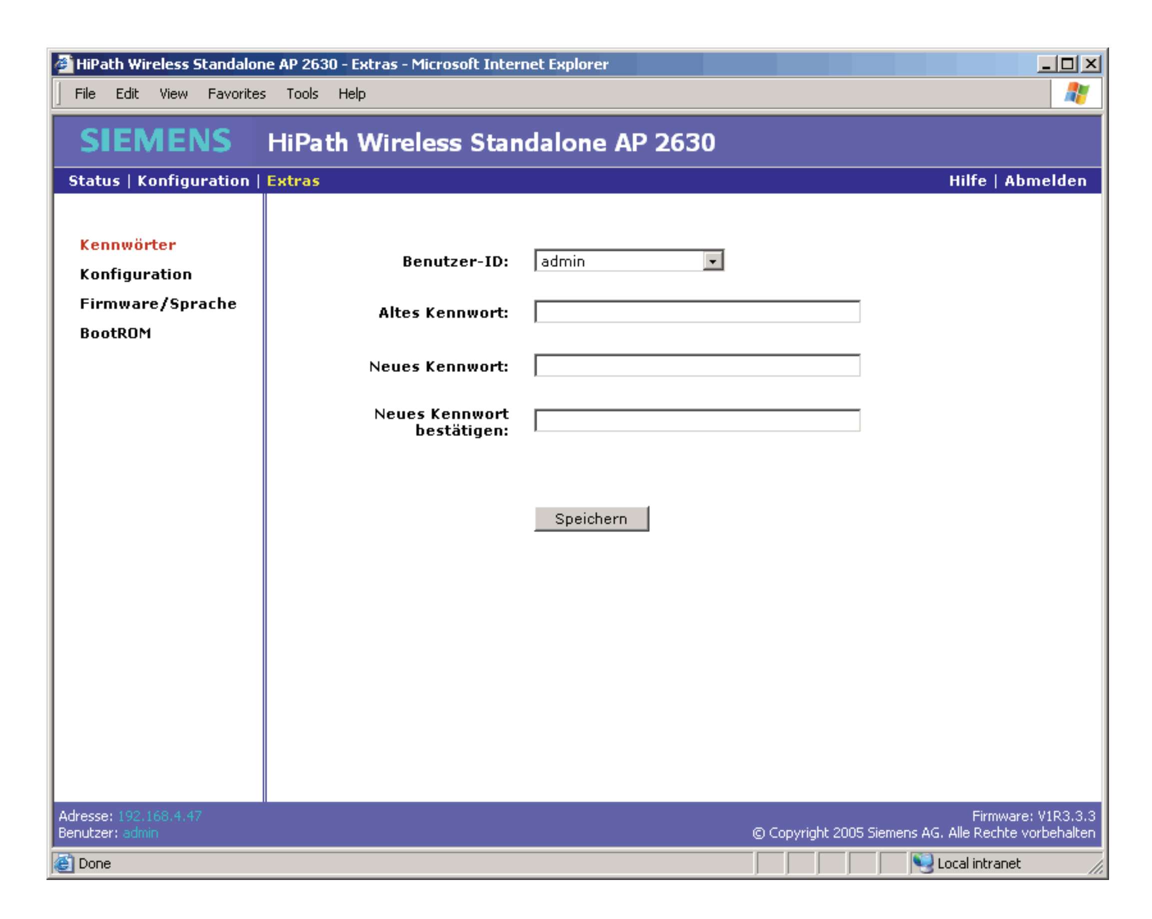


Zum Ändern eines Kennworts müssen Sie Administratorzugriff haben.

In der Dropdown-Liste **Benutzer-ID** können Sie zwischen einem Administrator und einem Standardbenutzer wählen. Um angemessene Sicherheit zu gewährleisten, muss das alte Kennwort für den gewählten Benutzer eingegeben werden, unabhängig davon, welcher Benutzer angemeldet ist und welche Benutzer-ID ausgewählt wurde.

So ändern Sie ein Kennwort:

1. Klicken Sie in der Menüleiste auf **Extras**.
2. Klicken Sie im linken Fenster auf **Kennwörter**.



3. Wählen Sie aus der Dropdown-Liste **Benutzer-ID** den Benutzer aus, dessen Kennwort Sie ändern wollen.

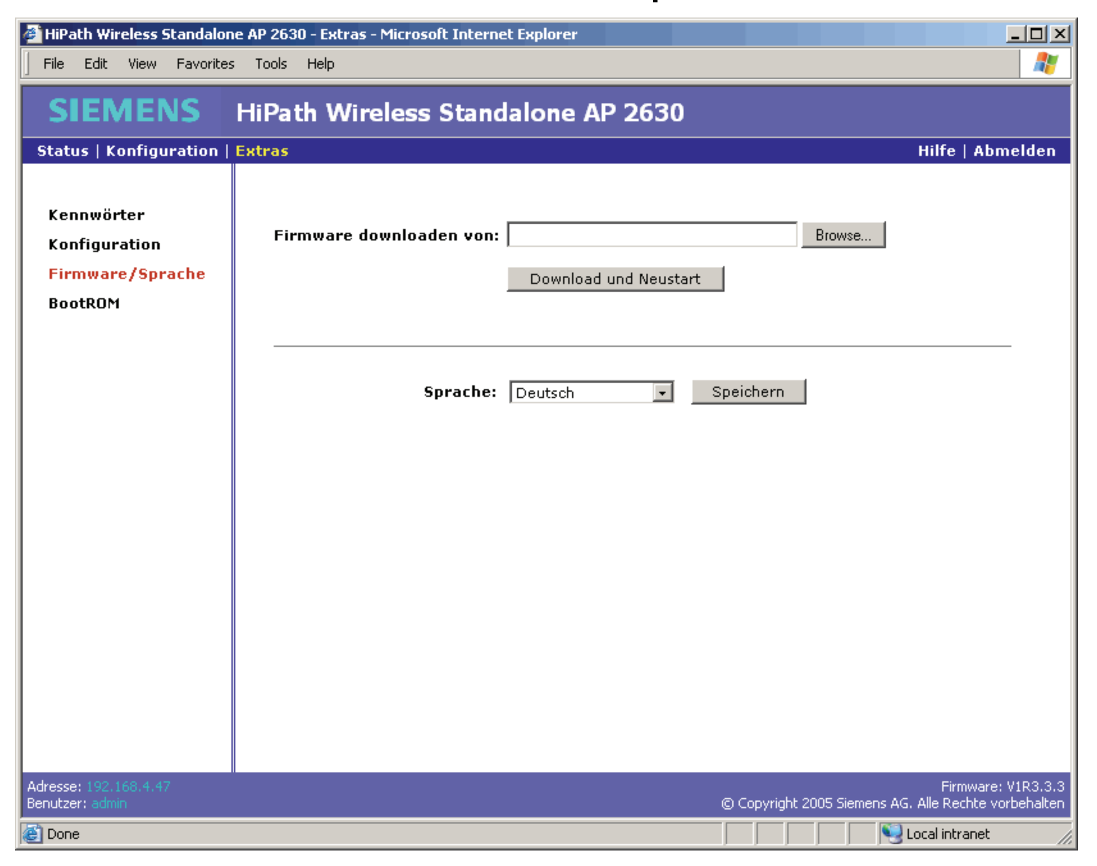
4. Geben Sie in das Feld **Altes Kennwort** das derzeit verwendete Kennwort ein.
5. Geben Sie in das Feld **Neues Kennwort** das neue Kennwort ein.
6. Geben Sie in das Feld **Neues Kennwort bestätigen** das neue Kennwort erneut ein.
7. Um Ihre Änderungen zu speichern, klicken Sie auf **Speichern**.

5.4 Herunterladen der Firmware

Verwenden Sie den Bildschirm **Firmware/Sprache**, um Firmware für den Standalone Access Point herunterzuladen.

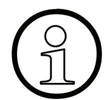
So laden Sie die Firmware herunter:

1. Klicken Sie in der Menüleiste auf **Extras**.
2. Klicken Sie im linken Fenster auf **Firmware/Sprache**.



3. Klicken Sie im Bereich **Firmware downloaden von** auf **Durchsuchen**, um zur entsprechenden Datei zu navigieren.

4. Wählen Sie die Datei aus, die heruntergeladen werden soll, und klicken Sie im Dialogfeld **Datei auswählen** auf **Öffnen**. Der Verzeichnispfad wird im Feld **Firmware downloaden von** angezeigt.
5. Klicken Sie auf **Download und Neustart**. Die ausgewählte Datei wird heruntergeladen, und der Standalone Access Point wird neu gestartet.



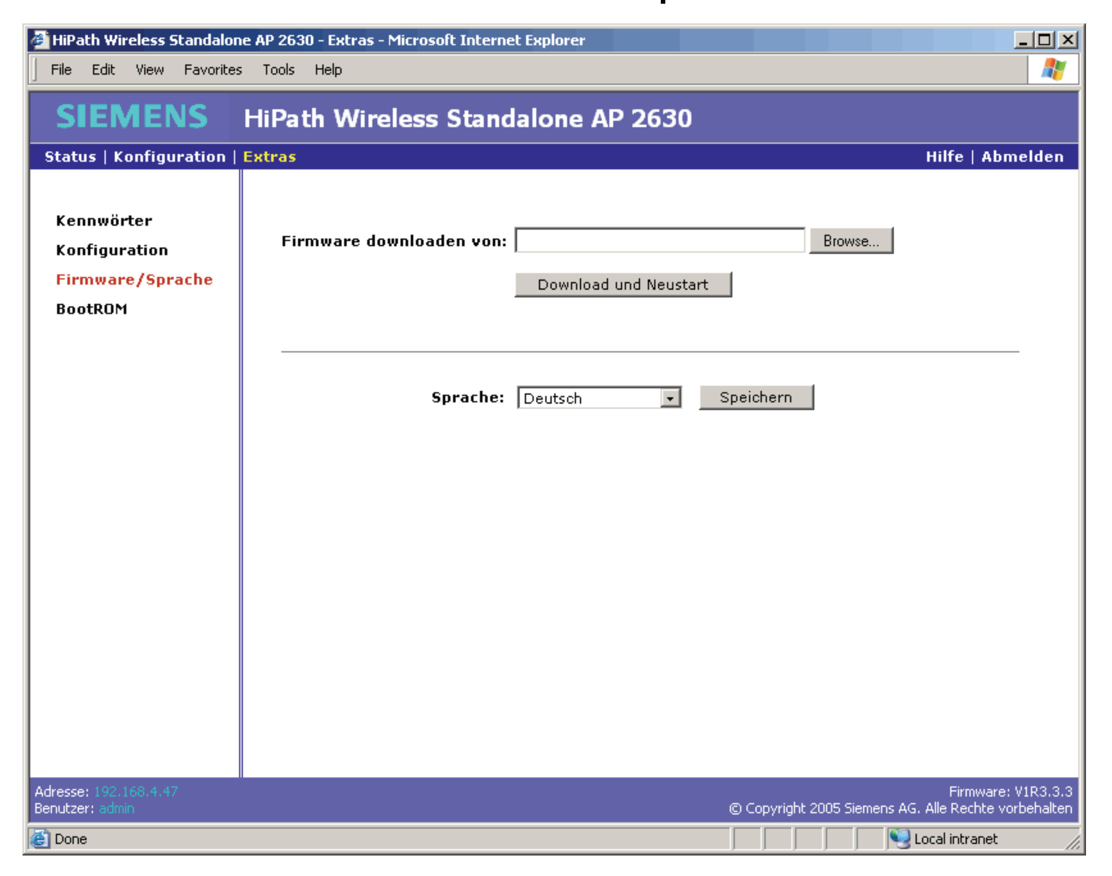
Der Standalone Access Point wird automatisch mit der eben heruntergeladenen Firmware-Version neu gestartet. Weitere Informationen finden Sie im Abschnitt 7.1, “Neustart”, auf Seite 103.

5.5 Einstellen der Oberflächensprache

Verwenden Sie den Bildschirm **Firmware/Sprache**, um die Oberflächensprache einzustellen.

So ändern Sie die Einstellung der Oberflächensprache:

1. Klicken Sie in der Menüleiste auf **Extras**.
2. Klicken Sie im linken Fenster auf **Firmware/Sprache**.



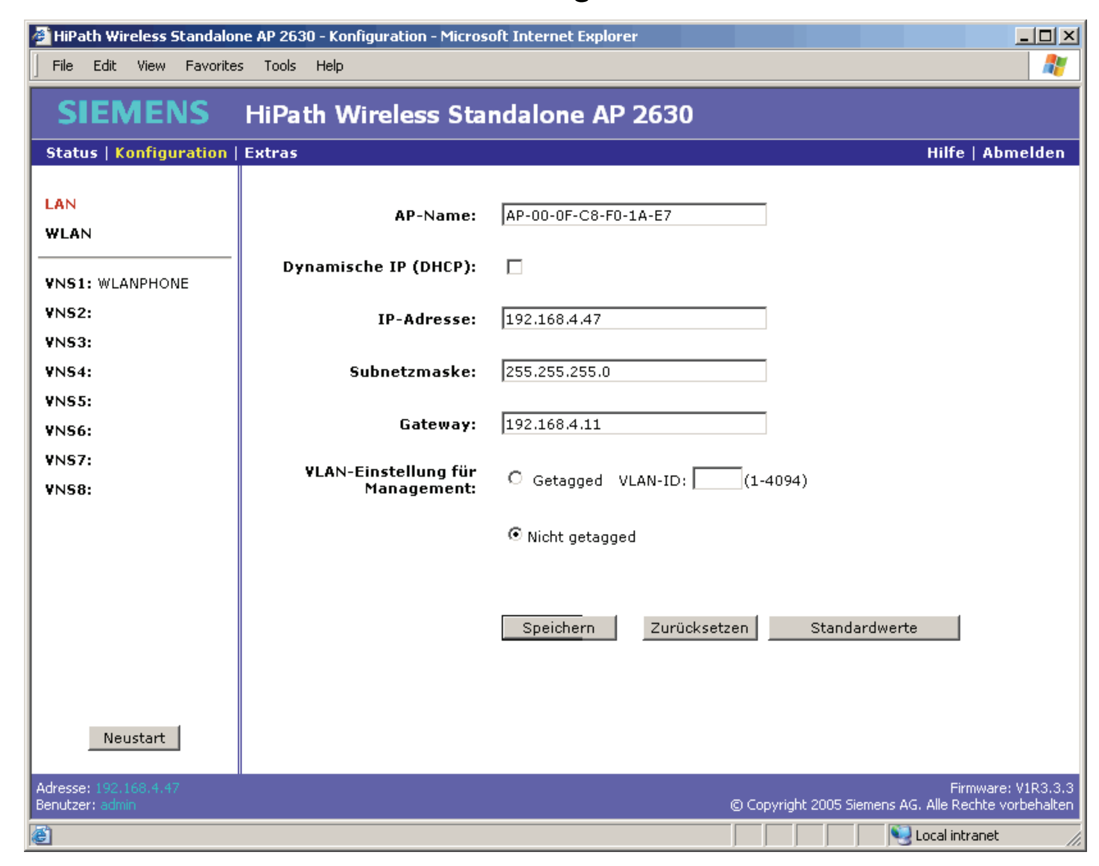
3. Wählen Sie in der Dropdown-Liste **Sprache** die gewünschte Sprache für die Benutzeroberfläche aus. Zur Auswahl stehen die Sprachen **Englisch** und **Deutsch**. Die Standardeinstellung ist **Englisch**.

5.6 Ändern der Host-IP-Adresse

Verwenden Sie den Bildschirm **LAN**, um die IP-Adresse für den Standalone Access Point zu ändern.

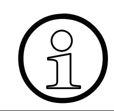
So ändern Sie die Host-IP-Adresse:

1. Klicken Sie in der Menüleiste auf **Konfiguration**. Der Bildschirm **LAN** wird angezeigt.



2. Geben Sie in das Feld **IP-Adresse** die zu verwendende statische IP-Adresse ein. Der Standardwert ist **192.168.1.20**.

3. Um Ihre Änderungen zu speichern, klicken Sie auf **Speichern**.



Die Schaltfläche **Neustart** steht in diesem Bildschirm zur Verfügung. Weitere Informationen finden Sie im Abschnitt 7.1, “Neustart”, auf Seite 103.

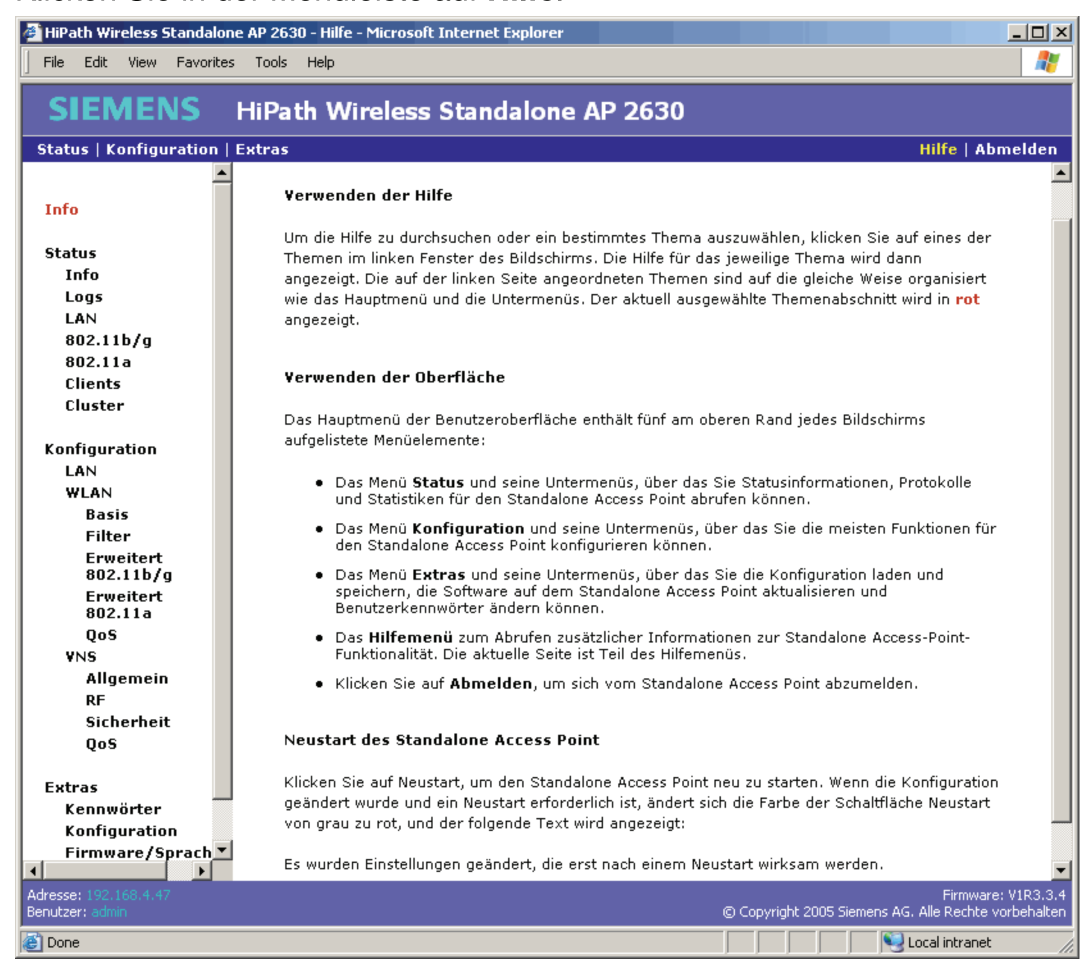
Weitere Details zu den LAN-Einstellungen in diesem Bildschirm finden Sie im Abschnitt 6.1, “Konfigurieren der LAN-Einstellungen”, auf Seite 67.

5.7 Zugreifen auf die Hilfefunktion

Verwenden Sie das Menü **Hilfe**, um zur Onlinehilfe zu gelangen.

So greifen Sie auf die Hilfefunktion zu:

1. Klicken Sie in der Menüleiste auf **Hilfe**.



2. Klicken Sie im linken Fenster auf das entsprechende Hilfethema. Die zugehörige Hilfeseite wird angezeigt.

6 Konfigurieren des Standalone Access Point



Es kann bis zu 60 Sekunden dauern, bis Konfigurationsänderungen im Compact-Flash-Speicher gespeichert werden. Wenn während dieses Zeitraums die Stromzufuhr unterbrochen wird, gehen die Konfigurationsänderungen verloren. Konfigurationsänderungen können ebenfalls verlorengehen, wenn die Stromversorgung für den Standalone Access Point zurückgesetzt wird, statt auf die **Neustart**-Schaltfläche zu klicken. Weitere Informationen finden Sie unter ”Neustart”, auf Seite 103.

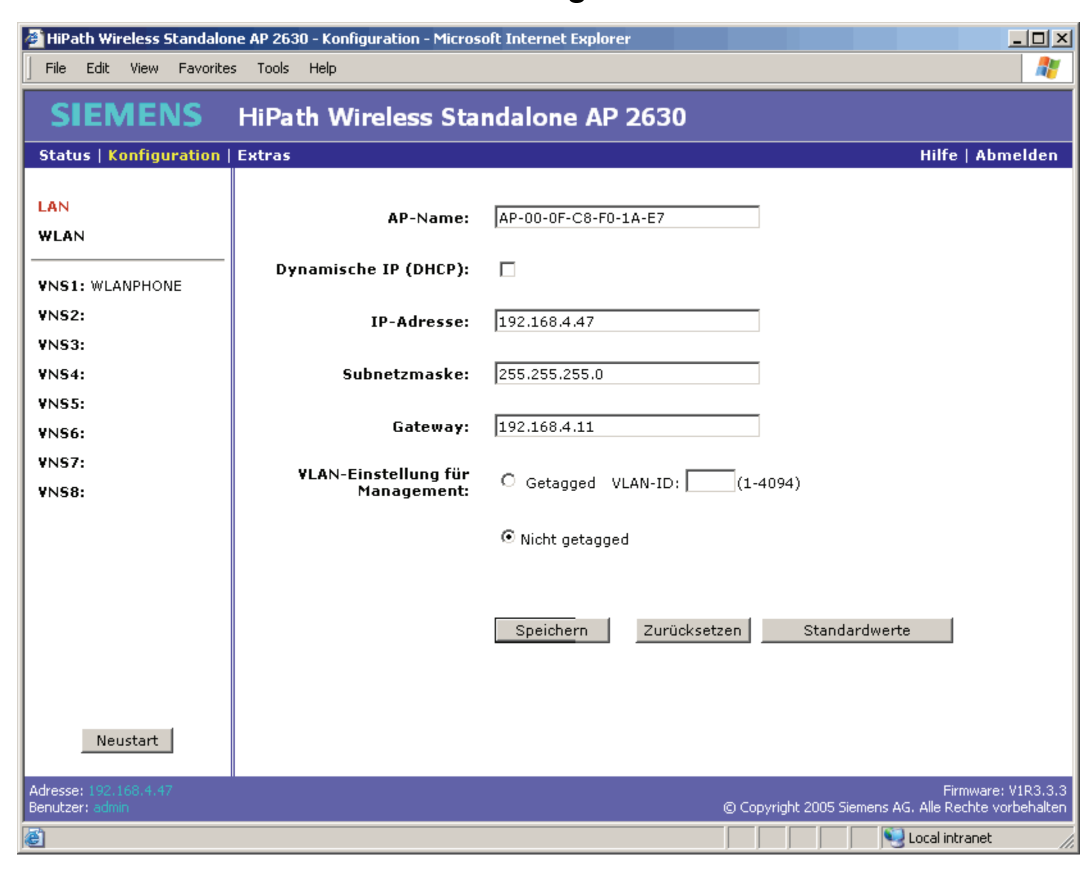
6.1 Konfigurieren der LAN-Einstellungen

Verwenden Sie den Bildschirm **LAN**, um die LAN-Konfiguration für den Standalone Access Point anzuzeigen und zu definieren, einschließlich der folgenden Informationen:

- Name des Access Point
- Dynamische oder statische IP-Adresse
- Statische IP-Einstellungen
- VLAN-Einstellung für Management

So konfigurieren Sie die LAN-Einstellungen:

1. Klicken Sie in der Menüleiste auf **Konfiguration**. Der Bildschirm **LAN** wird angezeigt.



2. Geben Sie im Feld **AP-Name** den Namen für den Access Point ein. Die Standardeinstellung ist AP-<MAC-Adresse>, wobei <MAC-Adresse> die MAC-Adresse ist.

3. Nehmen Sie eine der folgenden Einstellungen vor:

   - Um eine statische IP-Adresse zu verwenden, deaktivieren Sie das Kontrollkästchen **Dynamische IP (DHCP)**.

   - Um eine dynamische IP-Adresse zu verwenden, aktivieren Sie das Kontrollkästchen **Dynamische IP (DHCP)**. Standardmäßig ist das Kontrollkästchen aktiviert.

   Um eine statische IP-Adresse zu verwenden, gehen Sie wie folgt vor:

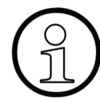
     - Geben Sie im Feld **IP-Adresse** die zu verwendende statische IP-Adresse ein. Der Standardwert ist **192.168.1.20**.

     - Geben Sie in das Feld **Subnetzmaske** die mit der zu verwendenden statischen IP-Adresse verbundene Subnetzmaske ein. Der Standardwert ist **255.255.255.0**.

     - Geben Sie in das Feld **Gateway** das mit der zu verwendenden statischen IP-Adresse verbundene Gateway ein. Der Standardwert ist **192.168.1.1**.

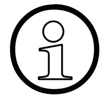
4. Nehmen Sie bei den Optionen unter VLAN-Einstellung für Management eine der folgenden Einstellungen vor:
   - **Getagged** - Wählen Sie diese Option, um alle IP Management-Pakete für diesen Standalone Access Point zu taggen.
     - **VLAN-ID** - Geben Sie den VLAN-ID-Wert ein, den Sie als Tag verwenden möchten.
   - **Nicht getagged** - Wählen Sie diese Option, um festzulegen, dass alle IP Management-Pakete für den Standalone Access Point nicht getagged sind. Die Standardeinstellung ist **Nicht getagged**.

   Für die VLAN-Aktivierung wird empfohlen, den Standalone Access Point zunächst in einer Umgebung ohne VLAN anzuschließen, das VLAN zu aktivieren, den Standalone Access Point in eine Umgebung zu verschieben, in der das VLAN erforderlich ist, und dann den Standalone Access Point neu zu starten. Die LAN-Konfiguration für den Standalone Access Point wird erst wirksam, nachdem der Standalone Access Point neu gestartet wurde. Daher kann auf den Standalone Access Point nur in einer Umgebung mit der korrekten VLAN-Einstellung zugegriffen werden.



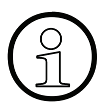
Wenn Sie den Standalone Access Point darauf konfigurieren, ein VLAN-Tag zu verwenden, müssen Sie sicherstellen, dass der Standalone Access Point mit einem Trunking Port verbunden ist. Die VLAN-Konfiguration auf dem Switch-Trunking-Port muss dieselbe VLAN-ID enthalten wie das auf dem Standalone Access Point konfigurierte VLAN-Tag.

5. Um Ihre Änderungen zu speichern, klicken Sie auf **Speichern**.



Eine Änderung der DHCP-, IP- oder VLAN-Einstellungen erfordert einen Neustart des Standalone Access Point. Die neuen Einstellungen werden erst nach abgeschlossenem Neustart wirksam. Durch Klicken auf **Speichern** wird die Verbindung nicht unterbrochen, während ein Neustart zu einer Verbindungsunterbrechung führen kann. Während des Neustarts wird folgende Meldung angezeigt:
Die IP/VLAN-Einstellung wurde geändert. Bitte melden Sie sich nach dem Neustart erneut an.

6. Um die in diesem Bildschirm angezeigten Einstellungen auf die zuletzt gespeicherten Werte zurückzusetzen, klicken Sie auf **Zurücksetzen**.
7. Um die Einstellungen auf diesem Bildschirm auf die werkseitigen Standardwerte zurückzusetzen, klicken Sie auf **Standardwerte**.



Die Schaltfläche **Neustart** steht in diesem Bildschirm zur Verfügung. Weitere Informationen finden Sie unter ”Neustart”, auf Seite 103.

6.2 Konfigurieren der WLAN-Einstellungen

Sie können die WLAN-Einstellungen für den Standalone Access Point konfigurieren. Während der Konfiguration der WLAN-Einstellungen für den Standalone Access Point ist Folgendes zu definieren:

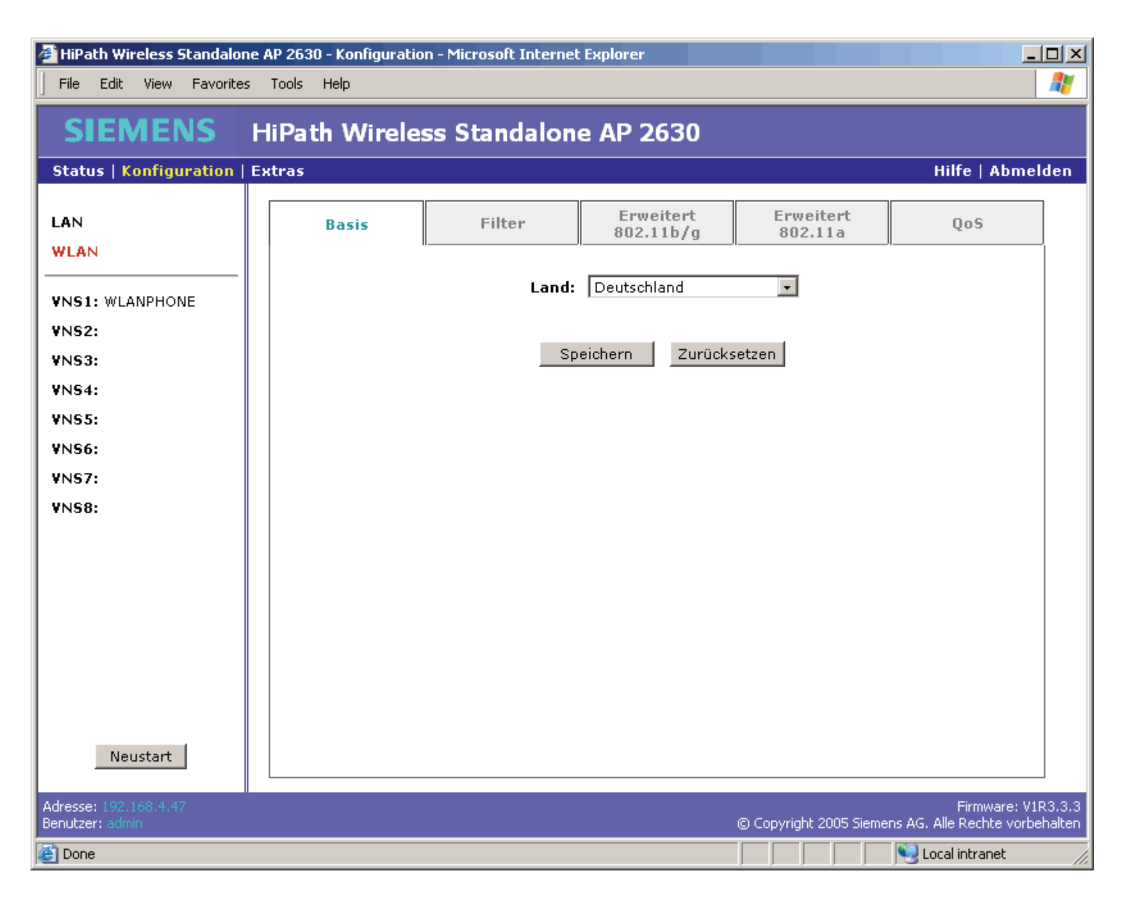
- Basiseinstellungen
- Filterkonfiguration
- 802.11b/g-Funkeinstellungen
- 802.11a-Funkeinstellungen
- QoS-Schwellwerte für Zugangskontrolle

6.2.1 Konfigurieren der WLAN-Basiseinstellungen

Verwenden Sie die Registerkarte **Basis**, um das Betriebsland für den Standalone Access Point auszuwählen.

So konfigurieren Sie die WLAN-Basiseinstellungen:

1. Klicken Sie in der Menüleiste auf **Konfiguration**.
2. Klicken Sie im linken Teilfenster auf **WLAN**. Die Registerkarte **Basis** wird angezeigt.

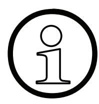


3. Wählen Sie aus der Dropdown-Liste **Land** das Betriebsland aus.

   Die korrekte Auswahl des Landes ist Voraussetzung für die Bereitstellung des passenden Dienstes. Zudem ist der Betrieb mit unkorrekter Ländereinstellung gesetzwidrig.

4. Um Ihre Änderungen zu speichern, klicken Sie auf **Speichern**.

5. Um die in diesem Bildschirm angezeigten Einstellungen auf die zuletzt gespeicherten Werte zurückzusetzen, klicken Sie auf **Zurücksetzen**.



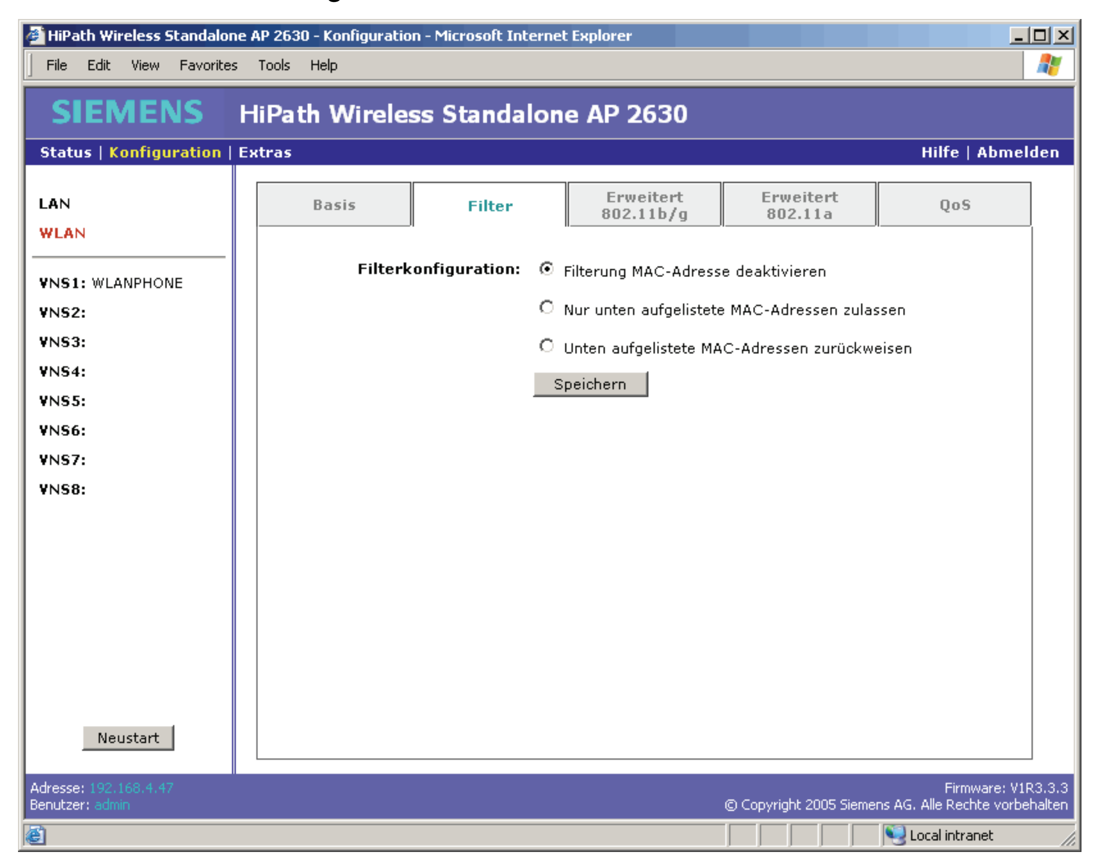
Die Schaltfläche **Neustart** steht in diesem Bildschirm zur Verfügung. Weitere Informationen finden Sie unter ”Neustart”, auf Seite 103.

6.2.2 Konfigurieren der WLAN-Filtereinstellungen

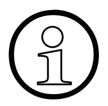
Verwenden Sie die Registerkarte **Filter**, um Client-Filterung basierend auf einer MAC-Adresse zu konfigurieren. Standardmäßig ist keine MAC-Adresse in der Liste und die Filterung der MAC-Adresse deaktiviert.

So konfigurieren Sie die Einstellungen für den WLAN-Filter:

1. Klicken Sie in der Menüleiste auf **Konfiguration**.
2. Klicken Sie im linken Teilfenster auf **WLAN**.
3. Klicken Sie auf die Registerkarte **Filter**.

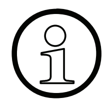


4. Wählen Sie im Bereich "Filterkonfiguration" eine der folgenden Vorgehensweisen:
   - **Filterung MAC-Adresse deaktivieren** - Wählen Sie diese Option, um die Filterung zu deaktivieren.
   - **Nur unten aufgelistete MAC-Adressen zulassen** - Wählen Sie diese Option, um die Verbindung nur für die in der Liste enthaltenen MAC-Adressen zuzulassen.
   - **Unten aufgelistete MAC-Adressen zurückweisen** - Wählen Sie diese Option, um die Verbindung für die aufgelisteten MAC-Adressen zurückzuweisen.



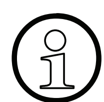
Die Filter Zulassen und Zurückweisen schließen sich gegenseitig aus. Sie können entweder eine Liste mit zugelassenen MAC-Adressen oder eine Liste mit zurückgewiesenen MAC-Adressen erstellen. Es ist nicht möglich, beide Listen gleichzeitig zu führen.

5. Um Ihre Änderungen zu speichern, klicken Sie auf **Speichern**.
6. Um eine Liste von zugelassenen bzw. zurückgewiesenen MAC-Adressen zu erstellen, geben Sie die neue MAC-Adresse im Feld **MAC-Adresse hinzufügen** ein, und klicken Sie auf **Hinzufügen**. Die Meldung **Update erfolgreich** wird angezeigt. Die neue MAC-Adresse wird in der Liste **MAC-Adresse** angezeigt, wenn Sie auf die entsprechende Option für die Filterkonfiguration klicken.



Falls erforderlich, klicken Sie auf **Auswahl zurücksetzen**, um alle aktivierten Kontrollkästchen in der Liste **MAC-Adresse** zu deaktivieren.

7. Um MAC-Adressen aus der Liste zu löschen, aktivieren Sie für jede der zu löschenden MAC-Adressen das Kontrollkästchen **Auswählen**, und klicken Sie dann auf **Ausgewählte Elemente löschen**. Die gelöschten MAC-Adressen werden aus der Liste MAC-Adresse entfernt.
8. Um alle MAC-Adressen aus der Liste zu löschen, klicken Sie auf **Alle löschen**. Alle MAC-Adressen werden aus der Liste MAC-Adresse entfernt.



Die Schaltfläche **Neustart** steht in diesem Bildschirm zur Verfügung. Weitere Informationen finden Sie unter ”Neustart”, auf Seite 103.

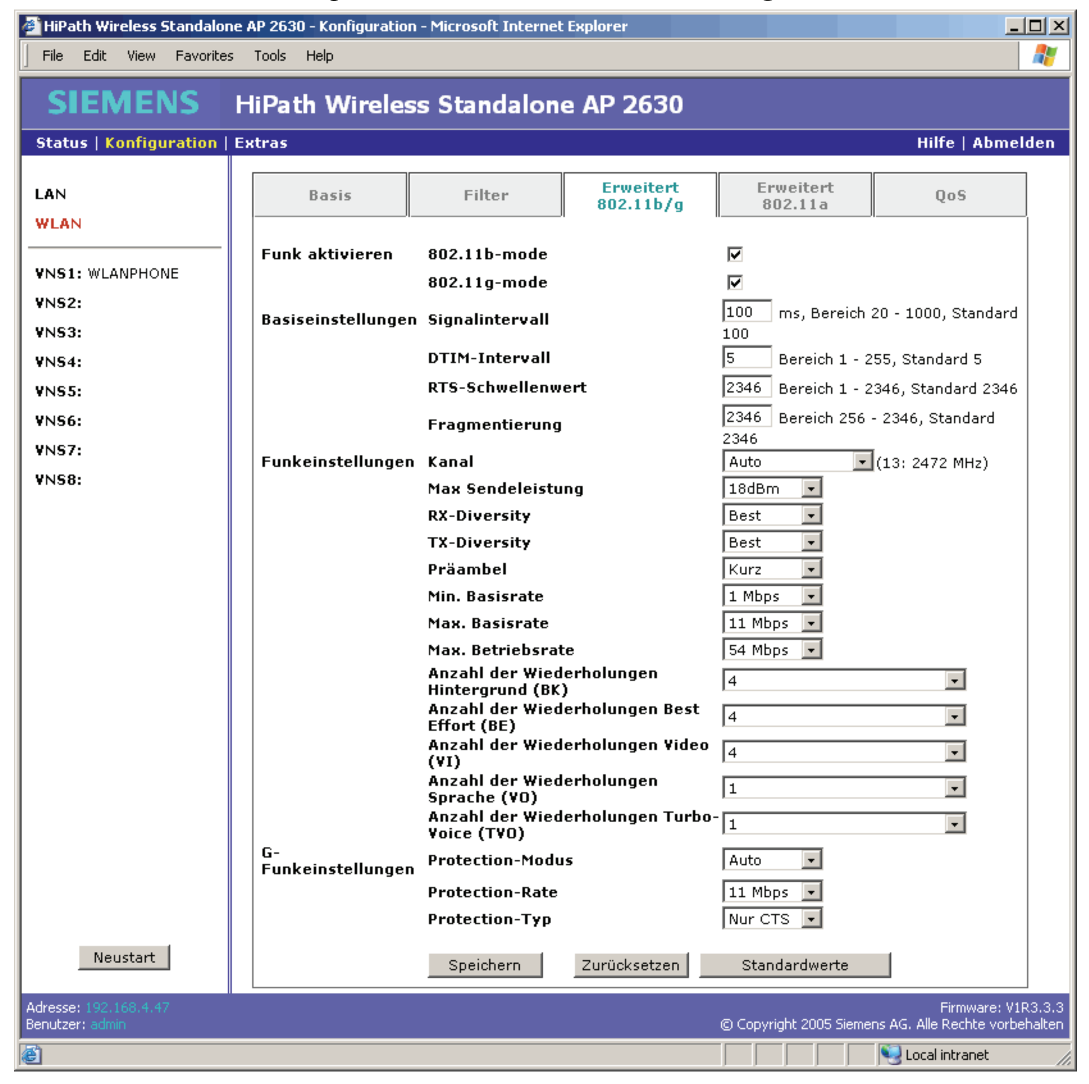
6.2.3 Konfigurieren der erweiterten 802.11b/g-Einstellungen

Verwenden Sie die Registerkarte **Erweitert 802.11b/g**, um die erweiterten 802.11b/g-Funkeinstellungen zu konfigurieren, einschließlich der folgenden Einstellungen:

- Steuerelemente zur Funkaktivierung
- Basiseinstellungen
- Funkeinstellungen
- G-Funkeinstellungen

So konfigurieren Sie die erweiterten 802.11b/g-Einstellungen:

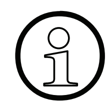
1. Klicken Sie in der Menüleiste auf **Konfiguration**.
2. Klicken Sie im linken Teilfenster auf **WLAN**.
3. Klicken Sie auf die Registerkarte **Erweitert 802.11b/g**.



4. Nehmen Sie im Bereich "Funk aktivieren" folgende Einstellungen vor:
   - **802.11b** - Wählen Sie diese Option, um den b/g-Funk für den Nur-b-Modus zu aktivieren.
   - **802.11g** - Wählen Sie diese Option, um den b/g-Funk für den Nur-g-Modus zu aktivieren.
   - Um den b/g-Funk für den Gemischt-Modus zu aktivieren, aktivieren Sie beide Kontrollkästchen **802.11b** und **802.11g**.

- Um den b/g-Funk zu deaktivieren, deaktivieren Sie beide Kontrollkästchen **802.11b** und **802.11g**.

5. Nehmen Sie im Bereich "Basiseinstellungen" folgende Einstellungen vor:
   - **Signalintervall** - Geben Sie das gewünschte Zeitintervall (in Millisekunden) zwischen Signalübertragungen ein. Die Standardeinstellung ist **100 Millisekunden**.
   - **DTIM-Intervall** - Geben Sie das gewünschte Intervall für die DTIM (Delivery Traffic Indication Map) ein, also die Anzahl der Signalintervalle zwischen zwei DTIM-Signalen. Um beim Client die Stromkosten zu minimieren, geben Sie eine große Zahl an, beispielsweise 5. Um die Broadcast- und Multicast-Verzögerung zu verringern, geben Sie eine kleine Zahl an. Der Standardwert ist **5**.
   - **RTS-Schwellenwert** - Geben Sie den Schwellwert für die Paketgröße in Bytes ein. Wenn dieser Wert überschritten wird, muss vor der Übertragung des Pakets ein RTS/CTS (Request to Send/Clear to Send)-Handshake durchgeführt werden. Der Standardwert ist **2346**, d.h. alle Pakete werden ohne RTS/CTS gesendet. Verringern Sie diesen Wert nur wenn unbedingt nötig.
   - **Fragmentierung** - Geben Sie hier den Schwellwert für die Paketgröße in Bytes ein, bei dessen Überschreitung, der Standalone Access Point die Pakete vor der Übertragung fragmentiert. Der Standardwert ist **2346**, d.h. alle Pakete werden ohne Fragmentierung gesendet. Verringern Sie diesen Wert nur wenn unbedingt nötig.
6. Nehmen Sie im Bereich "Funkeinstellungen" folgende Einstellungen vor:
   - **Kanal** - Wählen Sie den drahtlosen Kanal aus, den der Standalone Access Point für die Kommunikation mit drahtlosen Geräten verwenden soll. Je nach (landesabhängigem) Geltungsbereich können einige Kanäle eingeschränkt sein. Bei Auswahl der Option **Auto** wählt der Standalone Access Point den passenden Kanal automatisch aus. Wenn **Auto** ausgewählt wurde, wird der aktuell ausgewählte Kanal neben der Dropdown-Liste **Kanal** angezeigt. Die Standardeinstellung ist **Auto**.
   - **Max. Sendeleistung** - Wählen Sie die Sendeleistung (Tx-Power) für den Standalone Access Point: **8** bis **18 dBm**. Der Standardwert ist **18 dBm**.



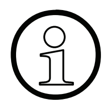
Verringern Sie die Einstellung für Tx-Power, wenn zwei oder mehr benachbarte Access Points auf demselben Kanal betrieben werden.

   - **RX-Diversity** - Wählen Sie **Best** für das beste Signal von beiden Antennen bzw. **Links** oder **Rechts**, um eine der beiden Diversity-Antennen auszuwählen. Die Standardauswahl (empfohlen) ist **Best**. Wenn nur eine Antenne angeschlossen ist, verwenden Sie die entsprechende Diversity-Einstellung **Links** oder **Rechts**. Verwenden Sie nicht **Best**, wenn nicht zwei identische Antennen verwendet werden.

- **TX-Diversity** - Wählen Sie **Best** für das beste Signal von beiden Antennen bzw. **Links** oder **Rechts**, um eine der beiden Diversity-Antennen auszuwählen. Die Standardauswahl ist **Best**, wodurch für die meisten Clients maximale Leistung erzielt wird. Einige Clients können jedoch bei der Einstellung **Best** für TX-Diversity ein ungewöhnliches Verhalten zeigen. In diesem Fall sollte für TX-Diversity entweder **Links** oder **Rechts** verwendet werden. Wenn nur eine Antenne angeschlossen ist, verwenden Sie die entsprechende Diversity-Einstellung **Links** oder **Rechts**. Verwenden Sie nicht **Best**, wenn nicht zwei identische Antennen verwendet werden.
- **Präambel** - Wählen Sie **Kurz**, um zuzulassen, dass jedes Paket weniger WLAN-Bandbreite nutzt, um so den Gesamtdurchsatz zu erhöhen, oder wählen Sie **Lang**, um besseren Schutz bereitzustellen. Die Standardeinstellung ist **Kurz**.
- **Min. Basisrate** - Wählen Sie die minimale Datenrate aus, die von allen Teilnehmern eines BSS unterstützt werden muss: **1**, **2**, **5,5** oder **11 Mbps** für 11b- und 11b+11g-Modus. Wählen Sie **1**, **2**, **5,5**, **6**, **11**, **12** oder **24 Mbps** für Nur-11g-Modus aus. Falls erforderlich, wird die Auswahl für die **Max. Basisrate** automatisch so angepasst, dass sie höher als die **Min. Basisrate** ist bzw. ihr entspricht; die Auswahl für die **Max. Betriebsrate** wird automatisch so angepasst, dass sie höher als die **Max. Basisrate** ist bzw. ihr entspricht. Wenn sowohl die **Min. Basisrate** als auch die **Max. Basisrate** auf eine 11g-spezifische (OFDM) Rate gesetzt sind, z.B. **6**, **12** oder **24 Mbps**, so sind alle Basisraten 11g-spezifisch.
- **Max. Basisrate** - Wählen Sie die maximale Datenrate aus, die von allen Teilnehmern eines BSS unterstützt werden muss: **1**, **2**, **5,5** oder **11 Mbps** für 11b- und 11b+11g-Modus. Wählen Sie **1**, **2**, **5,5**, **6**, **11**, **12** oder **24 Mbps** für Nur-11g-Modus aus. Falls erforderlich, wird die Auswahl für die **Max. Betriebsrate** automatisch so angepasst, dass sie höher als die **Max. Basisrate** ist bzw. ihr entspricht. Wenn sowohl die **Min. Basisrate** als auch die **Max. Basisrate** auf eine 11g-spezifische (OFDM) Rate gesetzt sind, z.B. **6**, **12** oder **24** Mbps, so sind alle Basisraten 11g-spezifisch.
- **Max. Betriebsrate** - Wählen Sie die maximale Datenrate aus, mit der die Clients arbeiten können, während sie mit dem Standalone Access Point verbunden sind: **1**, **2**, **5,5**, **11 Mbps** für den Nur-11b-Modus. Wählen Sie **1**, **2**, **5,5**, **6**, **9**, **11**, **12**, **18**, **24**, **36**, **48** oder **54 Mbps** für 11b+11g-Modus und Nur-11g-Modus aus. Falls erforderlich, wird die Auswahl für die **Max. Betriebsrate** automatisch so angepasst, dass sie höher als die **Max. Basisrate** ist bzw. ihr entspricht.
- **Anzahl der Wiederholungen Hintergrund (BK)** - Wählen Sie die Anzahl der Wiederholungen für die Übertragungswarteschlange im Hintergrund aus. Der Standardwert ist **4**. Die empfohlene Einstellung ist **anpassungsfähig (Multi-Rate)**.
- **Anzahl der Wiederholungen Best Effort (BE)** - Wählen Sie die Anzahl der Wiederholungen für die Übertragungswarteschlange Best Effort aus. Der Standardwert ist **4**. Die empfohlene Einstellung ist **anpassungsfähig (Multi-Rate)**.

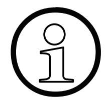
- **Anzahl der Wiederholungen Video (VI)** - Wählen Sie die Anzahl der Wiederholungen für die Übertragungswarteschlange Video aus. Der Standardwert ist **4**. Die empfohlene Einstellung ist **anpassungsfähig (Multi-Rate)**.
- **Anzahl der Wiederholungen Sprache (VO)** - Wählen Sie die Anzahl der Wiederholungen für die Übertragungswarteschlange Sprache aus. Der Standardwert ist **1**. Die empfohlene Einstellung ist **anpassungsfähig (Multi-Rate)**.
- **Anzahl der Wiederholungen Turbo-Voice (TVO)** - Wählen Sie die Anzahl der Wiederholungen für die Übertragungswarteschlange Turbo-Voice aus. Der Standardwert ist **1**. Die empfohlene Einstellung ist **anpassungsfähig (Multi-Rate)**.

7. Wenn für b/g-Funk der 802.11g-Modus aktiviert ist, gehen Sie wie folgt vor:
   - **Protection-Modus** - Wählen Sie einen Protection-Modus aus: **Keiner**, **Auto** oder **Immer**. Die Standardeinstellung (empfohlen) ist **Auto**. Wählen Sie **Keiner**, wenn voraussichtlich keine 11b-Access Points und -Clients beteiligt sein werden. Wählen Sie **Immer**, wenn voraussichtlich zahlreiche Nur-11b-Clients beteiligt sein werden.
   - **Protection-Rate** - Wählen Sie eine Protection-Rate aus: **1**, **2**, **5,5** oder **11 Mbps**. Die Standardeinstellung (empfohlen) ist **11 Mbps**. Verringern Sie die Rate nur, wenn sich in der Umgebung viele 11b-Clients befinden oder wenn es in einigen Bereichen des Systems Empfangsprobleme gibt. Beispielsweise können Raten unter 11 Mbps erforderlich sein, um den Empfang sicherzustellen.
   - **Protection-Typ** - Wählen Sie einen Protection-Typ aus: **Nur CTS** oder **RTS CTS**. Die Standardeinstellung (empfohlen) ist **Nur CTS**. Wählen Sie **RTS CTS** nur aus, wenn ein 11b-Access Point in der näheren Umgebung erkannt wird, der auf demselben Kanal betrieben wird, oder wenn sich viele Nur-11-Clients in der Umgebung befinden.



Für bestimmte Client-Karten oder -Anwendungen müssen möglicherweise die Standardeinstellungen geändert werden. Falls ja, gehen Sie nach den Anweisungen des Herstellers vor.

8. Um Ihre Änderungen zu speichern, klicken Sie auf **Speichern**.
9. Um die in diesem Bildschirm angezeigten Einstellungen auf die zuletzt gespeicherten Werte zurückzusetzen, klicken Sie auf **Zurücksetzen**.
10. Um die Einstellungen auf diesem Bildschirm auf die werkseitigen Standardwerte zurückzusetzen, klicken Sie auf **Standardwerte**.



Die Schaltfläche **Neustart** steht in diesem Bildschirm zur Verfügung. Weitere Informationen finden Sie unter ”Neustart”, auf Seite 103.

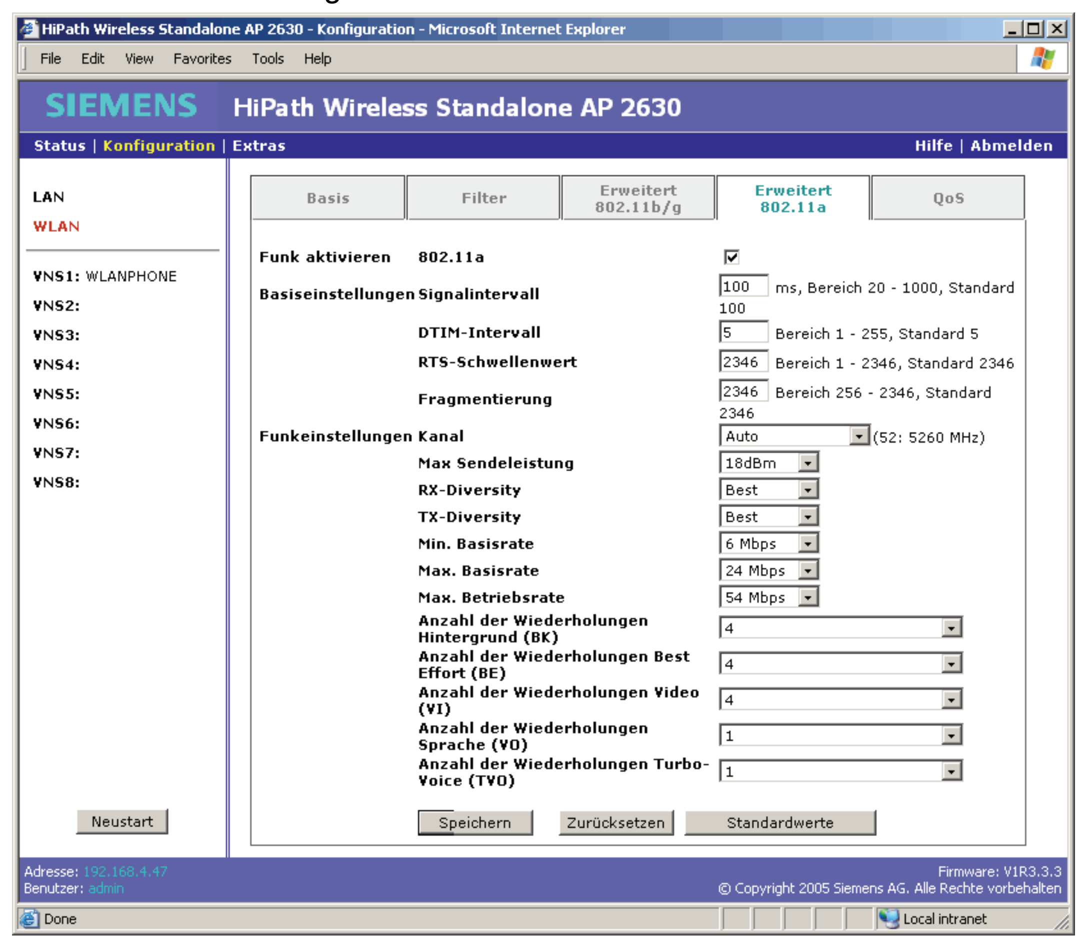
6.2.4 Konfigurieren der erweiterten 802.11a-Einstellungen

Verwenden Sie die Registerkarte **Erweitert 802.11a**, um die erweiterten 802.11a-Funkeinstellungen zu konfigurieren, einschließlich der folgenden Einstellungen:

- Steuerelemente zur Funkaktivierung
- Basiseinstellungen
- Funkeinstellungen

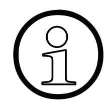
So konfigurieren Sie die erweiterten 802.11a-Einstellungen:

1. Klicken Sie in der Menüleiste auf **Konfiguration**.
2. Klicken Sie im linken Teilfenster auf **WLAN**.
3. Klicken Sie auf die Registerkarte **Erweitert 802.11a**.



4. Aktivieren Sie im Bereich "Funk aktivieren" das Kontrollkästchen **802.11a**, um das Funkmodul zu aktivieren. Deaktivieren Sie das Kontrollkästchen, um das Funkmodul auszuschalten. Standardmäßig ist das Kontrollkästchen aktiviert.

5. Nehmen Sie im Bereich "Basiseinstellungen" folgende Einstellungen vor:
   - **Signalintervall** - Geben Sie das gewünschte Zeitintervall (in Millisekunden) zwischen Signalübertragungen ein. Die Standardeinstellung ist **100 Millisekunden**.
   - **DTIM-Intervall** - Geben Sie das gewünschte Intervall für die DTIM (Delivery Traffic Indication Map) ein, also die Anzahl der Signalintervalle zwischen zwei DTIM-Signalen. Um beim Client die Stromkosten zu minimieren, geben Sie eine große Zahl an, beispielsweise 5. Um die Broadcast- und Multicast-Verzögerung zu verringern, geben Sie eine kleine Zahl an. Der Standardwert ist **5**.
   - **RTS-Schwellenwert** - Geben Sie den Schwellwert für die Paketgröße in Bytes ein. Wenn dieser Wert überschritten wird, muss vor der Übertragung des Pakets ein RTS/CTS (Request to Send/Clear to Send)-Handshake durchgeführt werden. Der Standardwert ist **2346**, d.h. alle Pakete werden ohne RTS/CTS gesendet. Verringern Sie diesen Wert nur wenn unbedingt nötig.
   - **Fragmentierung** - Geben Sie hier den Schwellwert für die Paketgröße in Bytes ein, bei dessen Überschreitung, der Standalone Access Point die Pakete vor der Übertragung fragmentiert. Der Standardwert ist **2346**, d.h. alle Pakete werden ohne Fragmentierung gesendet. Verringern Sie diesen Wert nur wenn unbedingt nötig.
6. Nehmen Sie im Bereich "Funkeinstellungen" folgende Einstellungen vor:
   - **Kanal** - Wählen Sie den drahtlosen Kanal aus, den der Wireless Access Point für die Kommunikation mit drahtlosen Geräten verwenden soll. Je nach (landesabhängigem) Geltungsbereich können einige Kanäle eingeschränkt sein. Die Standardeinstellung basiert auf Nordamerika. Bei Auswahl der Option **Auto** wählt der Standalone Access Point den passenden Kanal automatisch aus. Wenn **Auto** ausgewählt wurde, wird der zu verwendende Kanal neben der Dropdown-Liste **Kanal** angezeigt. Die Standardeinstellung ist **Auto**.
   - **Max. Sendeleistung** - Wählen Sie die Sendeleistung (Tx-Power) für den Standalone Access Point aus: **0** bis **18 dBm**. Der Standardwert ist **18 dBm**.

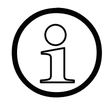


Verringern Sie die Einstellung für Tx-Power, wenn zwei oder mehr benachbarte Access Points auf demselben Kanal betrieben werden.

   - **RX-Diversity** - Wählen Sie **Best** für das beste Signal von beiden Antennen bzw. **Links** oder **Rechts**, um eine der beiden Diversity-Antennen auszuwählen. Die Standardauswahl (empfohlen) ist **Best**. Wenn nur eine Antenne angeschlossen ist, verwenden Sie die entsprechende Diversity-Einstellung **Links** oder **Rechts**. Verwenden Sie nicht **Best**, wenn nicht zwei identische Antennen verwendet werden.
   - **TX-Diversity** - Wählen Sie **Best** für das beste Signal von beiden Antennen bzw. **Links** oder **Rechts**, um eine der beiden Diversity-Antennen auszuwählen. Die Standardauswahl ist **Best**, wodurch für die meisten Clients maximale Leistung erzielt

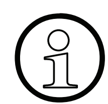
wird. Einige Clients können jedoch bei der Einstellung **Best**für TX-Diversity ein ungewöhnliches Verhalten zeigen. In diesem Fall sollte für TX-Diversity entweder **Links** oder **Rechts** verwendet werden. Wenn nur eine Antenne angeschlossen ist, verwenden Sie die entsprechende Diversity-Einstellung **Links** oder **Rechts**. Verwenden Sie nicht **Best**, wenn nicht zwei identische Antennen verwendet werden.

- **Min. Basisrate** - Wählen Sie die minimale Datenrate aus, die von allen Teilnehmern eines BSS unterstützt werden muss: **6**, **12** oder **24 Mbps**. Falls erforderlich, wird die Auswahl für die **Max. Basisrate** automatisch so angepasst, dass sie höher als die **Min. Basisrate** ist bzw. ihr entspricht; die Auswahl für die **Max. Betriebsrate** wird automatisch so angepasst, dass sie höher als die **Max. Basisrate** ist bzw. ihr entspricht.
- **Max. Basisrate** - Wählen Sie die maximale Datenrate aus, die von allen Teilnehmern eines BSS unterstützt werden muss: **6**, **12** oder **24 Mbps**. Falls erforderlich, wird die Auswahl für die **Max. Basisrate** automatisch so angepasst, dass sie höher als die **Min. Basisrate** ist bzw. ihr entspricht. Falls erforderlich, wird die Auswahl für die **Max. Betriebsrate** automatisch so angepasst, dass sie höher als die **Max. Basisrate** ist bzw. ihr entspricht.
- **Max. Betriebsrate** - Wählen Sie die maximale Datenrate aus, mit der die Clients arbeiten können, während sie mit dem Standalone Access Point verbunden sind: **6, 9, 12, 18, 24**, **36**, **48** oder **54 Mbps**. Falls erforderlich, wird die Auswahl für die **Max. Betriebsrate** automatisch so angepasst, dass sie höher als die **Max. Basisrate** ist bzw. ihr entspricht.
- **Anzahl der Wiederholungen Hintergrund (BK)** - Wählen Sie die Anzahl der Wiederholungen für die Übertragungswarteschlange im Hintergrund aus. Der Standardwert ist **4**. Die empfohlene Einstellung ist **anpassungsfähig (Multi-Rate)**.
- **Anzahl der Wiederholungen Best Effort (BE)** - Wählen Sie die Anzahl der Wiederholungen für die Übertragungswarteschlange Best Effort aus. Der Standardwert ist **4**. Die empfohlene Einstellung ist **anpassungsfähig (Multi-Rate)**.
- **Anzahl der Wiederholungen Video (VI)** - Wählen Sie die Anzahl der Wiederholungen für die Übertragungswarteschlange Video aus. Der Standardwert ist **4**. Die empfohlene Einstellung ist **anpassungsfähig (Multi-Rate)**.
- **Anzahl der Wiederholungen Sprache (VO)** - Wählen Sie die Anzahl der Wiederholungen für die Übertragungswarteschlange Sprache aus. Der Standardwert ist **1**. Die empfohlene Einstellung ist **anpassungsfähig (Multi-Rate)**.
- **Anzahl der Wiederholungen Turbo-Voice (TVO)** - Wählen Sie die Anzahl der Wiederholungen für die Übertragungswarteschlange Turbo-Voice aus. Der Standardwert ist **1**. Die empfohlene Einstellung ist anpassungsfähig (Multi-Rate).



Für bestimmte Client-Karten oder -Anwendungen müssen möglicherweise die Standardeinstellungen geändert werden. Falls ja, gehen Sie nach den Anweisungen des Herstellers vor.

7. Um Ihre Änderungen zu speichern, klicken Sie auf **Speichern**.
8. Um die in diesem Bildschirm angezeigten Einstellungen auf die zuletzt gespeicherten Werte zurückzusetzen, klicken Sie auf **Zurücksetzen**.
9. Um die Einstellungen auf dieser Registerkarte auf die werkseitigen Standardwerte zurückzusetzen, klicken Sie auf **Standardwerte**.



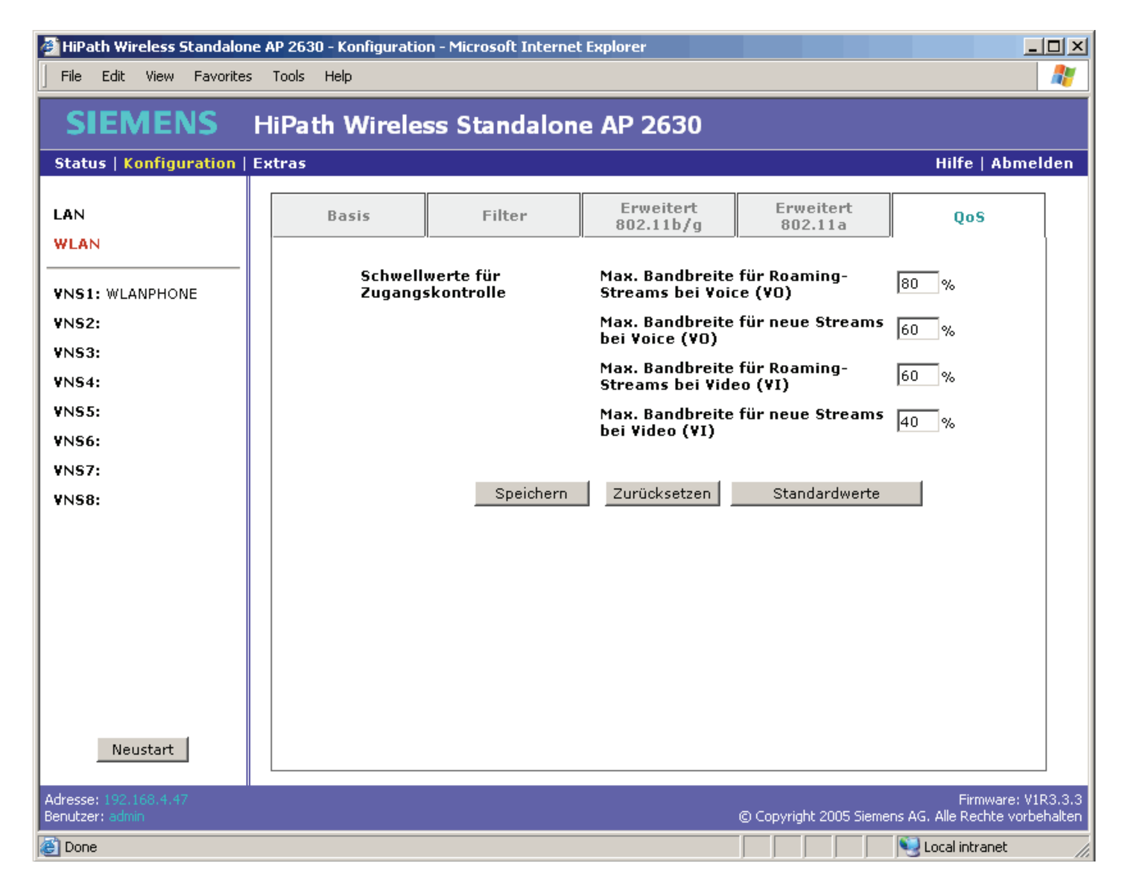
Die Schaltfläche **Neustart** steht in diesem Bildschirm zur Verfügung. Weitere Informationen finden Sie unter ”Neustart”, auf Seite 103.

6.2.5 Konfigurieren der WLAN-QoS-Einstellungen

Verwenden Sie die Registerkarte **QoS**, um die Schwellwerte für Zugangskontrolle anzuzeigen und zu definieren. Schwellwerte für Zugangskontrolle schützen zugelassenen Datenverkehr vor Überlastzuständen und stellen eindeutige Schwellwerte für VO und VI sowie für Roaming und neue Streams bereit.

So konfigurieren Sie die QoS-Einstellungen:

1. Klicken Sie in der Menüleiste auf **Konfiguration**.
2. Klicken Sie im linken Teilfenster auf **WLAN**.
3. Klicken Sie auf die Registerkarte **QoS**.

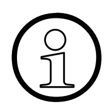


4. Definieren Sie unter Verwendung der Dropdown-Liste **Schwellwerte für Zugangskontrolle** die Schwellwerte für folgende Einstellungen:

   - **Max. Bandbreite für Roaming-Streams bei Voice (VO)** - Die maximal zulässige Gesamtbandbreite auf dem neuen Standalone Access Point, wenn ein Client mit einem aktiven Voice-Stream den Zugang für den Voice-Stream beantragt. Der Standardwert ist **80%**.
   - **Max. Bandbreite für neue Streams bei Voice (VO)** - Die maximal zulässige Gesamtbandbreite auf dem Standalone Access Point, wenn ein bereits verbundener Client den Zugang für einen neuen Voice-Stream beantragt. Der Standardwert ist **60%**.
   - **Max. Bandbreite für Roaming-Streams bei Video (VI)** - Die maximal zulässige Gesamtbandbreite auf dem Standalone Access Point, wenn ein Client mit einem aktiven Video-Stream den Zugang für den Video-Stream beantragt. Der Standardwert ist **60%**.
   - **Max. Bandbreite für neue Streams bei Video (VI)** - Die maximal zulässige Gesamtbandbreite auf dem Access Point, wenn ein bereits verbundener Client den Zugang für einen neuen Video-Stream beantragt. Der Standardwert ist **40%**.

5. Um Ihre Änderungen zu speichern, klicken Sie auf **Speichern**.

6. Um die in diesem Bildschirm angezeigten Einstellungen auf die zuletzt gespeicherten Werte zurückzusetzen, klicken Sie auf **Zurücksetzen**.
7. Um die Einstellungen auf dieser Registerkarte auf die werkseitigen Standardwerte zurückzusetzen, klicken Sie auf **Standardwerte**.



Die Schaltfläche **Neustart** steht in diesem Bildschirm zur Verfügung. Weitere Informationen finden Sie unter ”Neustart”, auf Seite 103.

6.3 Konfigurieren von VNS für den Standalone Access Point

Der Standalone Access Point kann bis zu 8 VNS unterstützen. Für jeden VNS können folgende Einstellungen konfiguriert werden:

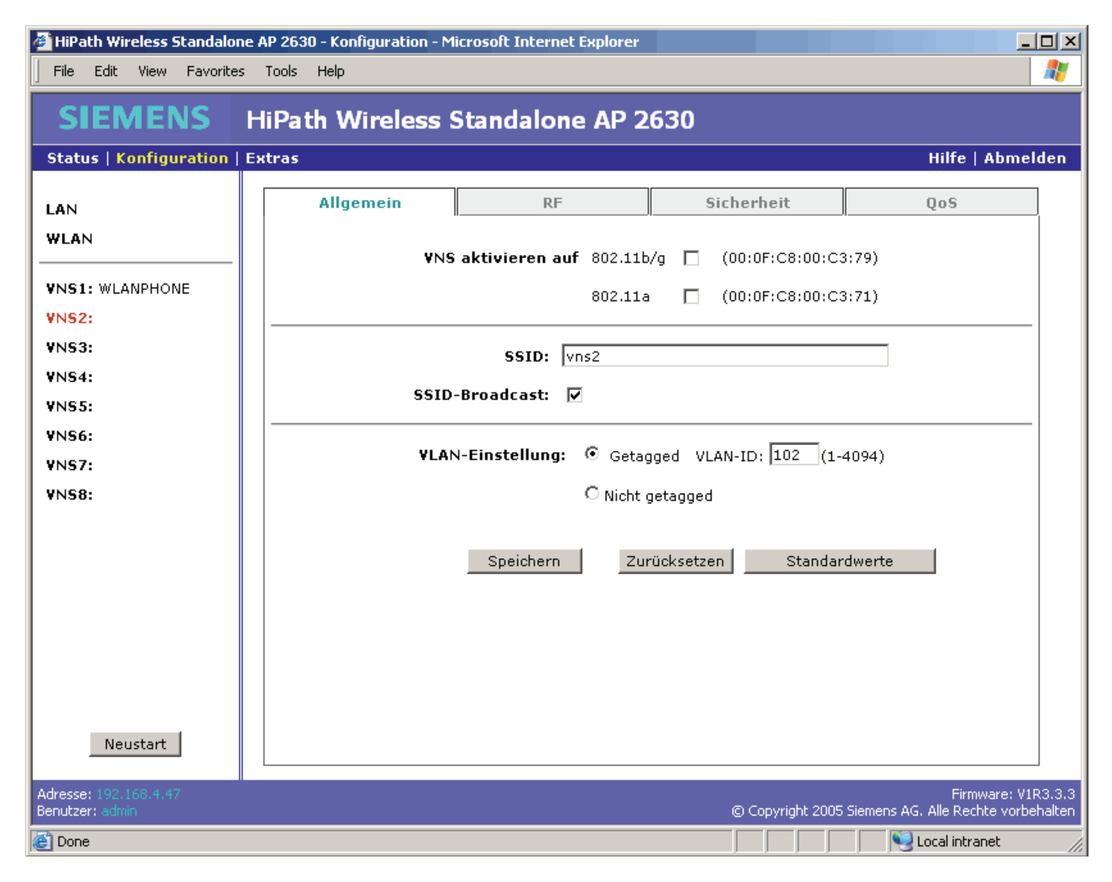
- Funkaktivierung
- SSID-Informationen
- VLAN-Einstellungen
- Funkfrequenz
- Sicherheitszuweisung
- Quality of Service

6.3.1 Einrichten der allgemeinen VNS-Konfiguration

Verwenden Sie die Registerkarte **Allgemein**, um die Funk-, SSID- und VLAN-Einstellungen für einen VNS zu konfigurieren. Die SSID für den ersten VNS ist standardmäßig WLANPHONE; dieser VNS ist aktiviert, während alle anderen VNS deaktiviert sind.

So konfigurieren Sie die allgemeinen Einstellungen für VNS:

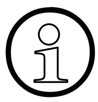
1. Klicken Sie in der Menüleiste auf **Konfiguration**.
2. Doppelklicken Sie im linken Fenster auf den VNS, den Sie konfigurieren möchten. Die Registerkarte **Allgemein** wird angezeigt.



3. Gehen Sie im Bereich "VNS aktivieren auf" wie folgt vor:
   - **802.11b/g** - Wählen Sie diese Option, um den VNS für 802.11b/g-Funk zu aktivieren.
   - **802.11a** - Wählen Sie diese Option, um den VNS für 802.11a-Funk zu aktivieren.
4. Geben Sie in das Feld **SSID** den Namen für den VNS ein.
5. Nehmen Sie eine der folgenden Einstellungen vor:
   - Um SSID-Broadcasting durch den Standalone Access Point zu aktivieren, aktivieren Sie das Kontrollkästchen **SSID-Broadcast**. Standardmäßig ist das Kontrollkästchen aktiviert.
   - Um SSID-Broadcasting durch den Standalone Access Point zu deaktivieren, deaktivieren Sie das Kontrollkästchen **SSID-Broadcast**.
6. Nehmen Sie bei den Optionen unter VLAN-Einstellung eine der folgenden Einstellungen vor:
   - **Getagged** - Wählen Sie diese Option, um alle IP-Pakete für diesen VNS zu taggen. Die Standardeinstellung ist **Getagged**.
     - **VLAN-ID** - Geben Sie den VLAN-ID-Wert ein, den Sie als Tag verwenden möchten.

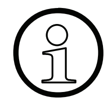
- **Nicht getagged** - Wählen Sie diese Option, um festzulegen, dass alle IP-Pakete für den VNS nicht getagged sind. Die Standardeinstellung ist **Nicht getagged**.

Standardmäßig ist der erste VNS **nicht getagged**, und die weiteren VNS sind **getagged**.



- Wenn Sie den Standalone Access Point darauf konfigurieren, ein VLAN-Tag zu verwenden, müssen Sie sicherstellen, dass der Standalone Access Point mit einem Trunking Port verbunden ist. Die VLAN-Konfiguration auf dem Switch-Trunking-Port muss dieselbe VLAN-ID enthalten wie das auf dem Standalone Access Point konfigurierte VLAN-Tag.
- Jede VLAN-ID muss für jeden VNS einmalig vergeben werden. Nur die VLAN-ID **VLAN-Einstellung für Management** kann mehrmals vergeben werden.

7. Um Ihre Änderungen zu speichern, klicken Sie auf **Speichern**.
8. Um die in diesem Bildschirm angezeigten Einstellungen auf die zuletzt gespeicherten Werte zurückzusetzen, klicken Sie auf **Zurücksetzen**.
9. Um die Einstellungen auf dieser Registerkarte auf die werkseitigen Standardwerte zurückzusetzen, klicken Sie auf **Standardwerte**.



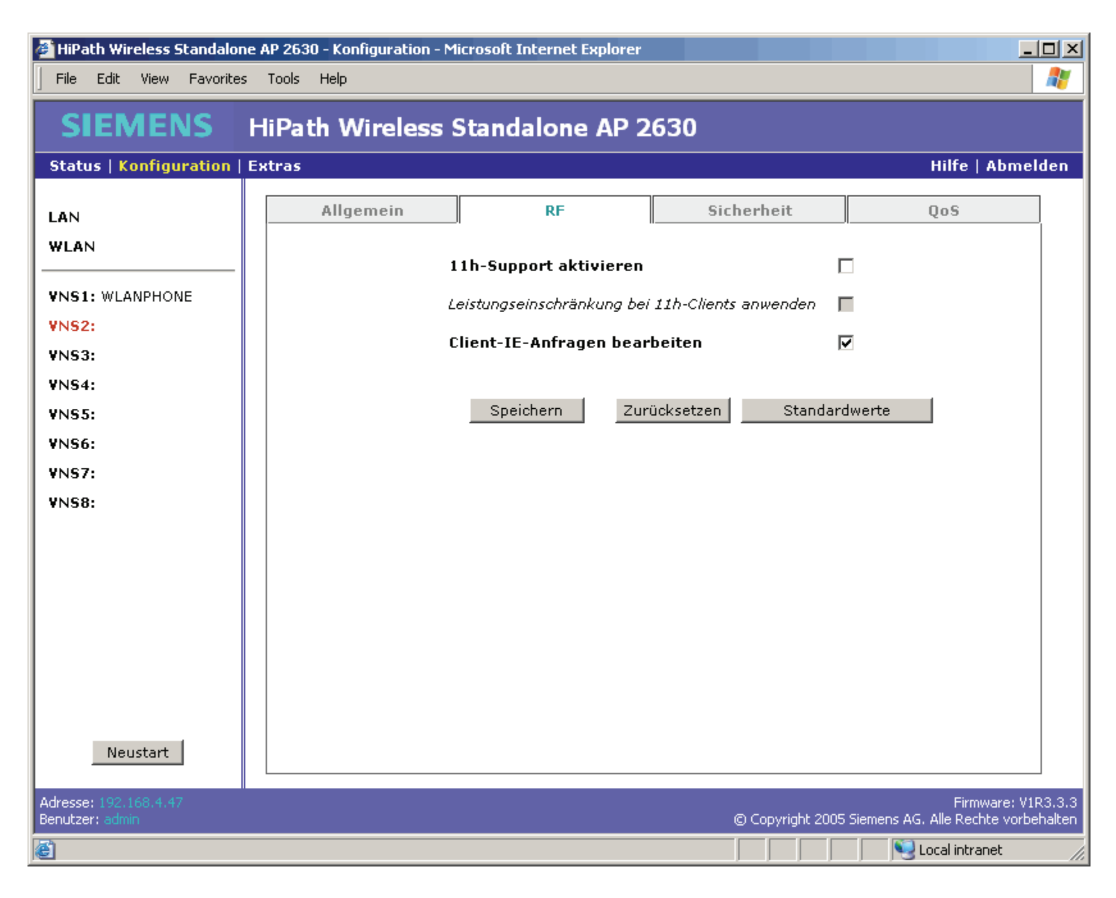
Die Schaltfläche **Neustart** steht in diesem Bildschirm zur Verfügung. Weitere Informationen finden Sie unter ”Neustart”, auf Seite 103.

6.3.2 Konfigurieren von Einstellungen für die VNS-Funkfrequenz

Verwenden Sie die Registerkarte **RF**, um die Einstellungen für die VNS-Funkfrequenz zu konfigurieren.

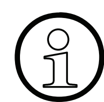
So konfigurieren Sie die VNS-Funkfrequenz:

1. Klicken Sie in der Menüleiste auf **Konfiguration**.
2. Doppelklicken Sie im linken Fenster auf den VNS, den Sie konfigurieren möchten.
3. Klicken Sie auf die Registerkarte **RF**.



4. Nehmen Sie folgende Einstellungen vor:
   - **11h-Support aktivieren** - Wählen Sie diese Option, um für diesen VNS 802.11h-Support zu aktivieren. Standardmäßig ist das Kontrollkästchen deaktiviert. Es wird empfohlen, diese Option zu aktivieren.
   - **Leistungseinschränkung bei 11h-Clients anwenden** - Wählen Sie diese Option, um für die mit diesem VNS verbundenen 11h-Clients die Anwendung eingeschränkter Leistung zu ermöglichen. Standardmäßig ist das Kontrollkästchen deaktiviert. Es wird empfohlen, diese Option zu aktivieren.
   - **Client-IE-Anfragen bearbeiten** - Wählen Sie diese Option, um dem Standalone Access Point zu ermöglichen, von Clients über Probe Request-Frames gesendete IE-Anforderungen zu akzeptieren und zu antworten, indem die angeforderten IEs in die entsprechenden Probe Response-Frames für diesen VNS eingefügt werden. Standardmäßig ist das Kontrollkästchen aktiviert. Es wird empfohlen, diese Option zu aktivieren.
5. Um Ihre Änderungen zu speichern, klicken Sie auf **Speichern**.
6. Um die in diesem Bildschirm angezeigten Einstellungen auf die zuletzt gespeicherten Werte zurückzusetzen, klicken Sie auf **Zurücksetzen**.

7. Um die Einstellungen auf dieser Registerkarte auf die werkseitigen Standardwerte zurückzusetzen, klicken Sie auf **Standardwerte**.



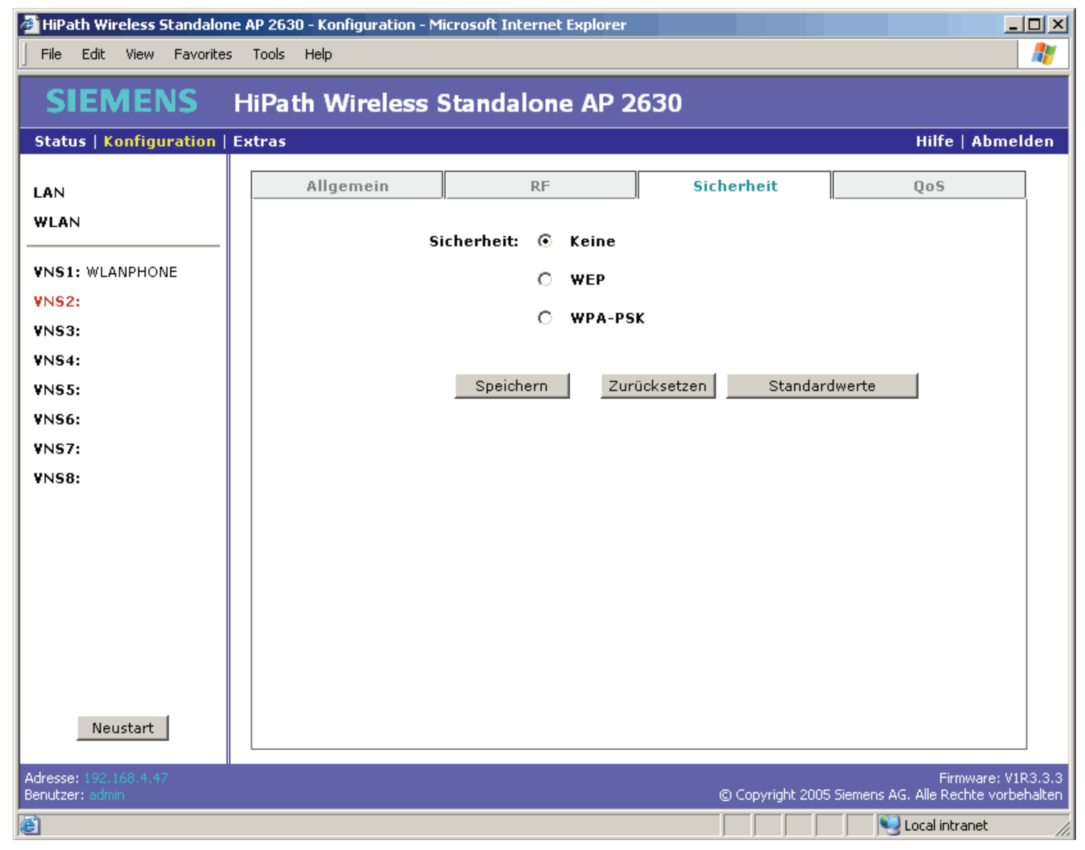
Die Schaltfläche **Neustart** steht in diesem Bildschirm zur Verfügung. Weitere Informationen finden Sie unter "Neustart", auf Seite 103.

6.3.3 Konfigurieren von VNS-Sicherheitseinstellungen

Verwenden Sie die Registerkarte **Sicherheit**, um die VNS-Sicherheit zu konfigurieren.

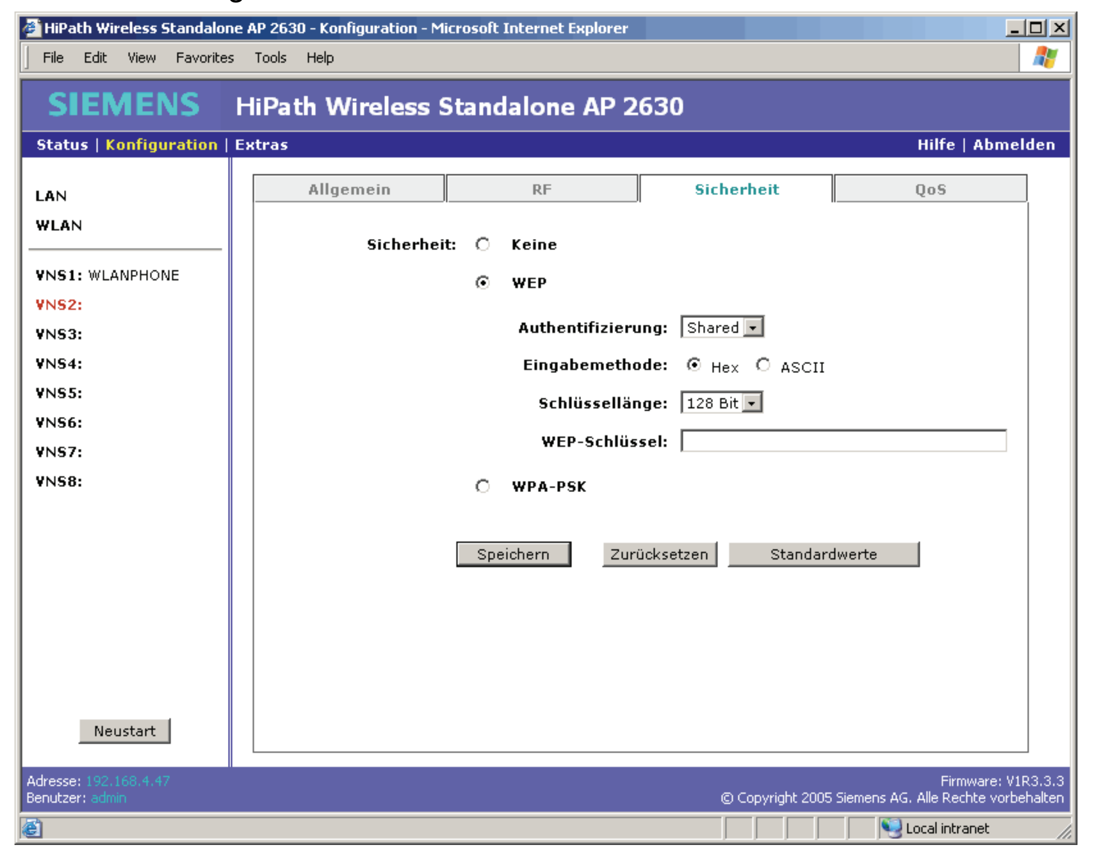
So konfigurieren Sie die VNS-Sicherheit:

1. Klicken Sie in der Menüleiste auf **Konfiguration**.
2. Doppelklicken Sie im linken Fenster auf den VNS, den Sie konfigurieren möchten.
3. Klicken Sie auf die Registerkarte **Sicherheit**.



4. Um die VNS-Sicherheit zu konfigurieren, nehmen Sie eine der folgenden Einstellungen vor:

   - **Keine** - Wählen Sie diese Option, um die Sicherheit zu deaktivieren. Die Standardeinstellung ist **Keine**.
   - **WEP** - Wählen Sie diese Option, um WEP (Static Wired Equivalent Privacy) als Sicherheitsprotokoll für den VNS zu aktivieren. Bei Auswahl der WEP-Sicherheit können Authentifizierungstyp, Eingabemethode, Schlüssellänge und der WEP-Schlüssel konfiguriert werden.

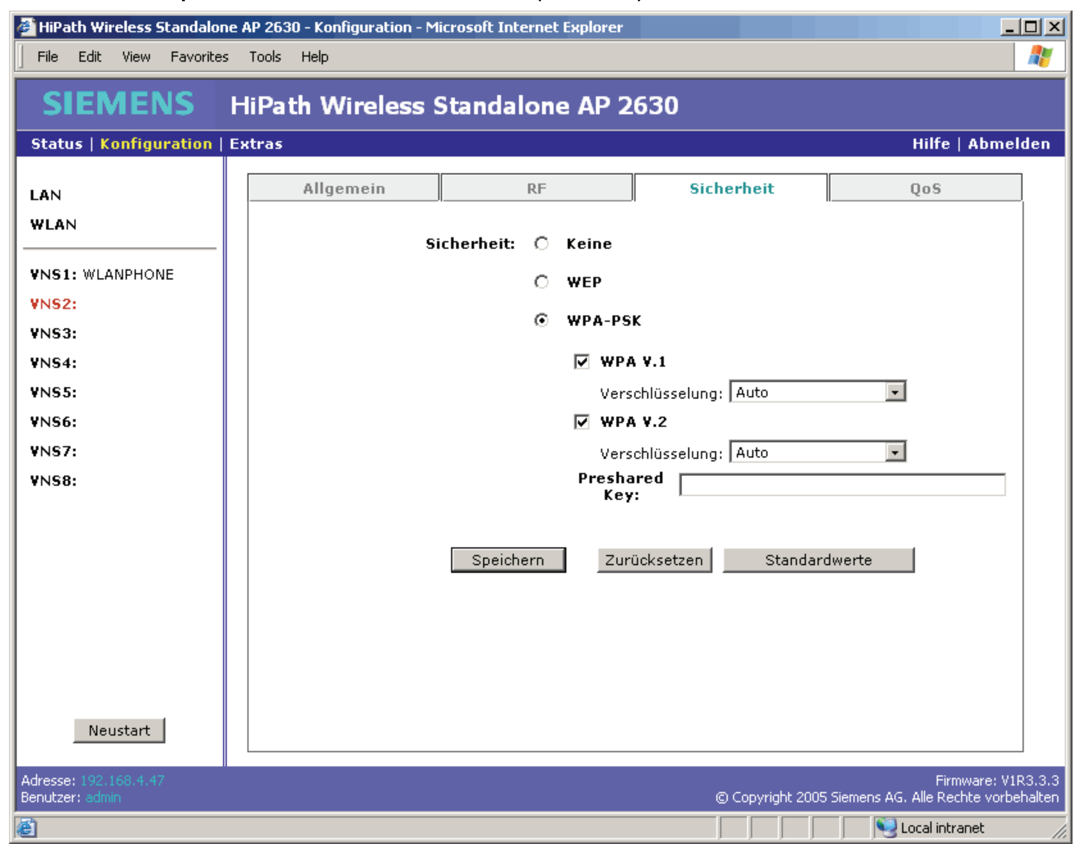


- **Authentifizierung** - Wählen Sie den zu verwendenden Authentifizierungstyp aus. Die verfügbaren Authentifizierungstypen sind **Open** (keine Authentifizierung), **Shared** (Preshared Key wird für Authentifizierung verwendet) und **Auto** (Open- oder Shared-Authentifizierung wird akzeptiert). Die Standardeinstellung ist **Shared**.
- Um die Eingabemethode festzulegen, wählen Sie **Hex** für einen Schlüssel im Hexadezimal-Format oder **ASCII** für einen Schlüssel im ASCII-Format. Die Standardeinstellung ist **Hex**.
- **Schlüssellänge** - Wählen Sie die Länge (in Bits) des Schlüssels aus. Die verfügbaren Schlüssellängen sind **40**, **104** und **128**. Der Standardwert ist **128**.

  - **WEP-Schlüssel** - Geben Sie den Schlüssel ein. Format und Länge des Schlüssels werden überprüft, wenn Sie Ihre Änderungen speichern.

- **WPA-PSK** - Wählen Sie diese Option, um WPA-PSK (Wi-Fi Protected Access Preshared Key) als Sicherheitsprotokoll für den VNS zu aktivieren. Bei Auswahl der WPA-PSK-Sicherheit können WPA V.1, WPA V.2 und der Preshared Key konfiguriert werden. Sie können WPA V.1 und WPA V.2 gleichzeitig aktivieren, damit unterschiedliche Clients mit WPA V.1 oder WPA V.2 verbunden werden können.

  WPA-PSK ergänzt die erweiterte WEP-Verschlüsselung und die Schlüsselverwaltung um die Komponente Authentifizierung. Im WPA-PSK-Modus ist die Angabe eines Authentifizierungsservers nicht erforderlich. Dieser Modus eignet sich für Heimarbeitsplätze oder kleine Büros (SOHO).



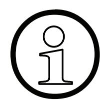
  - **WPA V.1** - Wählen Sie diese Option, um den Lösungsmodus vor 802.11i zuzulassen. Standardmäßig ist das Kontrollkästchen aktiviert.

  - **Verschlüsselung** - Wählen Sie den Verschlüsselungstyp **Auto** oder **Nur TKIP**. Die Standardeinstellung ist **Auto**. Wenn **Auto** ausgewählt wird, kündigt der Standalone Access Point sowohl TKIP als auch CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) für WPA V.1 an. CCMP ist ein IEEE 802.11i-Verschlüsselungsprotokoll, das die Verschlüsselungsmethode AES (Advanced Encryption Standard) verwendet.

Wenn **Nur TKIP** ausgewählt wird, kündigt der Standalone Access Point TKIP als verfügbares Verschlüsselungsprotokoll für WPA V.1 an. CCMP wird nicht angekündigt.

- **WPA V.2** - Wählen Sie diese Option, um den 802.11i-Lösungsmodus zuzulassen. Standardmäßig ist das Kontrollkästchen aktiviert.
- **Verschlüsselung** - Wählen Sie den Verschlüsselungstyp **Auto** oder **Nur AES**. Die Standardeinstellung ist **Auto**. Wenn **Auto** ausgewählt wird, kündigt der Standalone Access Point sowohl TKIP als auch CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) für WPA V.2 an. CCMP ist ein IEEE 802.11i-Verschlüsselungsprotokoll, das die Verschlüsselungsmethode AES (Advanced Encryption Standard) verwendet. Wenn **Nur AES** ausgewählt wird, kündigt der Standalone Access Point AES als verfügbares Verschlüsselungsprotokoll für WPA V.2 an. TKIP wird nicht angekündigt.
- **Preshared Key** - Geben Sie das zum Generieren des Schlüssels verwendete ASCII-Kennwort ein.

5. Um Ihre Änderungen zu speichern, klicken Sie auf **Speichern**.
6. Um die in diesem Bildschirm angezeigten Einstellungen auf die zuletzt gespeicherten Werte zurückzusetzen, klicken Sie auf **Zurücksetzen**.
7. Um die Einstellungen auf dieser Registerkarte auf die werkseitigen Standardwerte zurückzusetzen, klicken Sie auf **Standardwerte**.



Die Schaltfläche **Neustart** steht in diesem Bildschirm zur Verfügung. Weitere Informationen finden Sie unter ”Neustart”, auf Seite 103.

6.3.4 Konfigurieren von VNS-QoS-Einstellungen

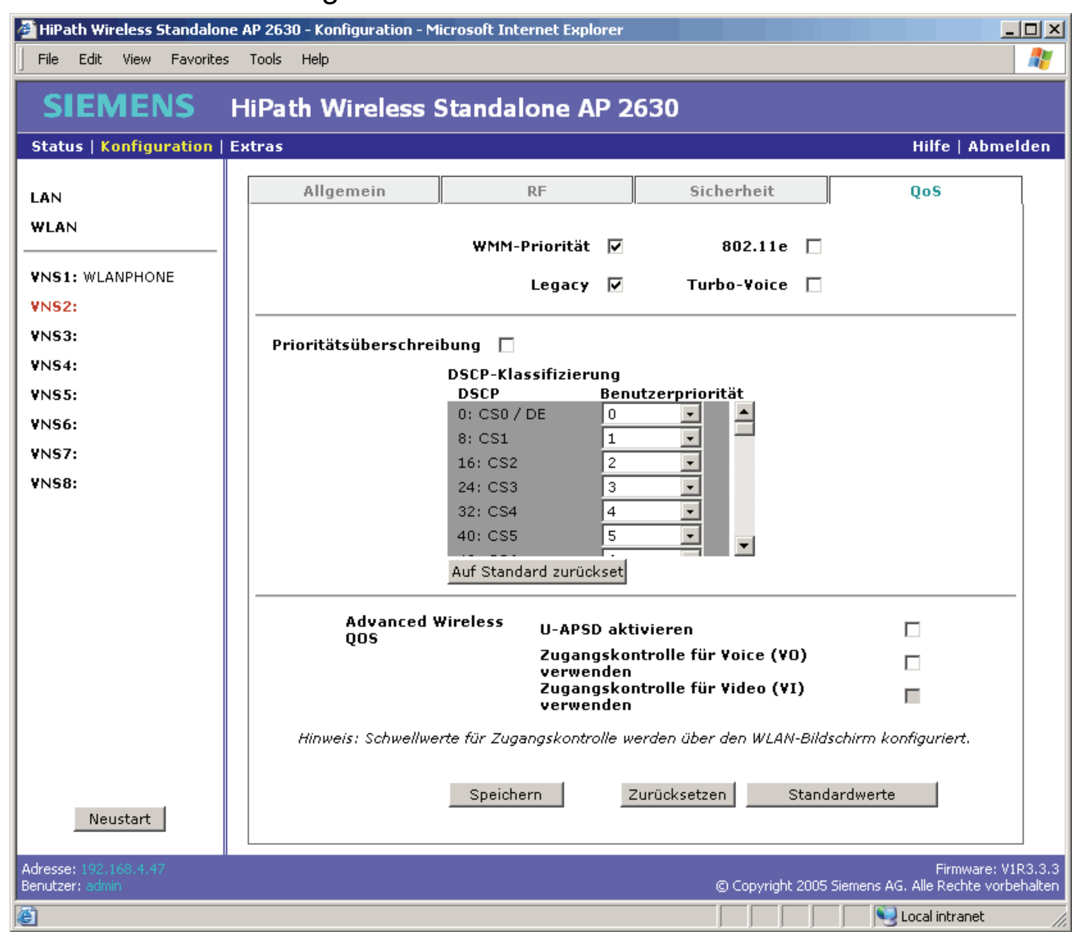
Verwenden Sie die Registerkarte **QoS**, um die VNS-QoS-Einstellungen zu konfigurieren. Die Registerkarte ermöglicht die QoS-Konfiguration und enthält u.a. folgende Informationen:

- **WMM-Priorität** - Wenn diese Option aktiviert ist, akzeptiert der Standalone Access Point WMM-Client-Verbindungen und übernimmt die Einstufung und Priorisierung des Downlink-Verkehrs für alle WMM-Clients. WMM-Clients übernehmen auch die Einstufung und Priorisierung des Uplink-Verkehrs.
- **802.11e** - Wenn diese Option aktiviert ist, akzeptiert der Standalone Access Point 802.11e-Client-Verbindungen und übernimmt die Einstufung und Priorisierung des Downlink-Verkehrs für alle 802.11e-Clients. Die 802.11e-Clients übernehmen auch die Einstufung und Priorisierung des Uplink-Verkehrs. WMM ist der von der WiFi Alliance eingerichtete Standard vor 802.11e.

- **Legacy** - Wenn diese Option aktiviert ist, übernimmt der Standalone Access Point die Einstufung und Priorisierung des Downlink-Verkehrs für alle Clients nach den bei WMM und 802.11e verwendeten Regeln.
- **Turbo-Voice** - Wenn einer der o.g. QoS-Modi aktiviert ist, ist auch der Turbo-Voice-Modus verfügbar. Wenn diese Option aktiviert ist, wird dem Sprachverkehr in diesem VNS eine höhere Priorität als dem Sprachverkehr in anderen VNS zugewiesen. Wenn Turbo-Voice zusammen mit WMM oder 802.11e aktiviert ist, werden die WMM- und/oder 802.11e-Clients in diesem VNS durch den Standalone Access Point angewiesen, den gesamten als Sprache eingestuften Verkehr mit speziellen Parametern zu übertragen, die der Optimierung der Übertragungsleistung und -kapazität dienen.

So konfigurieren Sie VNS-QoS-Einstellungen:

1. Klicken Sie in der Menüleiste auf **Konfiguration**.
2. Doppelklicken Sie im linken Fenster auf den VNS, den Sie konfigurieren möchten.
3. Klicken Sie auf die Registerkarte **QoS**.



4. Nehmen Sie folgende Einstellungen vor:

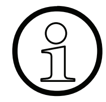
- **WMM-Priorität** - Wählen Sie diese Option, um festzulegen, dass der Standalone Access Point WMM-Client-Verbindungen akzeptiert und die Einstufung und Priorisierung des Downlink-Verkehrs für alle WMM-Clients übernimmt. WMM-Clients übernehmen auch die Einstufung und Priorisierung des Uplink-Verkehrs. WMM ist Bestandteil des 802.11e-Standards für QoS. Wenn diese Option gewählt wird, ist die Option **Turbo-Voice** verfügbar.
- **Legacy** - Wählen Sie diese Option, wenn Ihr VNS Legacy-Geräte unterstützt, die weder WMM noch 802.11e für die Priorisierung von Voice-Verkehr unterstützen. Wenn diese Option gewählt wird, ist die Option **Turbo-Voice** verfügbar.
- **802.11e** - Wählen Sie diese Option, um festzulegen, dass der Standalone Access Point 802.11e-Client-Verbindungen akzeptiert und die Einstufung und Priorisierung des Downlink-Verkehrs für alle 802.11e-Clients übernimmt. Die 802.11e-Clients übernehmen auch die Einstufung und Priorisierung des Uplink-Verkehrs. Wenn diese Option gewählt wird, ist die Option **Turbo-Voice** verfügbar.
- **Turbo-Voice** - Wählen Sie diese Option, um dem Sprachverkehr in diesem VNS eine höhere Priorität als dem Sprachverkehr in anderen VNS zuzuweisen. Wenn Turbo-Voice zusammen mit WMM oder 802.11e aktiviert ist, werden die WMM- und/oder 802.11e-Clients in diesem VNS durch den Standalone Access Point angewiesen, den gesamten als Sprache eingestuften Verkehr mit speziellen Parametern zu übertragen, die der Optimierung der Übertragungsleistung und -kapazität dienen. Die Option **Turbo-Voice** ist nur verfügbar, wenn eine der Optionen **WMM**, **802.11e** oder **Legacy** gewählt wurde.

5. Nehmen Sie eine der folgenden Einstellungen vor:
   - Aktivieren Sie das Kontrollkästchen **Prioritätsüberschreibung**, um den Prioritätslevel für den VNS zu definieren. Die Dropdownliste **Benutzerpriorität** wird angezeigt. Wählen Sie aus der Dropdown-Liste **Benutzerpriorität** den entsprechenden Prioritätslevel aus. Sie können einen der acht Prioritätslevel auswählen:
     - 7, 6 - Voice-Verkehr
     - 5, 4 - Video-Verkehr
     - 3, 0 - Best Effort
     - 2, 1 - Hintergrundverkehr
   - Wenn Sie jeder DSCP-Markierung einen Prioritätslevel zuweisen möchten, deaktivieren Sie das Kontrollkästchen **Prioritätsüberschreibung**, und definieren Sie die DSCP-COS-Prioritäten in der Tabelle **DSCP-Klassifizierung**.

     Verwenden Sie die Tabelle **DSCP-Klassifizierung**, um Downlink-Verkehr zu klassifizieren, indem der IP-DSCP der speziellen Benutzerpriorität zugeordnet wird, die für jeden IP-DSCP-Wert definiert ist. Wenn jedoch Prioritätsüberschreibung aktiviert ist, wird stattdessen die konfigurierte Benutzerpriorität verwendet.

Die letzte Benutzerpriorität bestimmt die Übertragungswarteschlange und die Benutzerpriorität für die WLAN QoS-Pakete (WMM oder 802.11e) in der Downlink-Richtung. Der Wert für Benutzerpriorität dient auch zum Taggen des Felds VLAN-Priorität für den Uplink-Verkehr, wenn für diesen VNS VLAN-Tagging aktiviert ist. Der Standalone Access Point überschreibt weder in der Downlink- noch in der Uplink-Richtung den DSCP im IP-Header des Benutzerpakets.

6. Die **Advanced Wireless QoS**-Optionen werden nur angezeigt, wenn die Kontrollkästchen **WMM-Priorität** oder **802.11e** aktiviert sind:
   - **U-APSD aktivieren** - Wählen Sie diese Option, um die Funktion Unscheduled Automatic Power Save Delivery (U-APSD) zu aktivieren. Diese Funktion kann von mobilen Geräten verwendet werden, um im Energiesparmodus effizient ein oder mehrere Echtzeit-Streams aufrechtzuerhalten. Diese Funktion funktioniert zusammen mit WMM und/oder 802.11e und wird automatisch deaktiviert, wenn sowohl WMM als auch 802.11e deaktiviert sind.
   - **Globale Zugangskontrolle für Voice (VO) verwenden** - Wählen Sie diese Option, um Zugangskontrolle für Voice zu aktivieren. Durch Aktivierung der Zugangskontrolle werden Clients gezwungen, einen Zugang zu beantragen, um die Hochpriorität-Zugriffskategorien in Downlink- und in Uplink-Richtung verwenden zu können. Die Zugangskontrolle schützt zugelassenen Datenverkehr vor neuen Bandbreitenanforderungen.
   - **Globale Zugangskontrolle für Video (VI) verwenden** - Diese Funktion ist nur verfügbar, wenn Zugangskontrolle für Voice aktiviert ist. Wählen Sie diese Option, um Zugangskontrolle für Video zu aktivieren. Durch Aktivierung der Zugangskontrolle werden Clients gezwungen, einen Zugang zu beantragen, um die Hochpriorität-Zugriffskategorien in Downlink- und in Uplink-Richtung verwenden zu können. Die Zugangskontrolle schützt zugelassenen Datenverkehr vor neuen Bandbreitenanforderungen.
7. Um Ihre Änderungen zu speichern, klicken Sie auf **Speichern**.
8. Um die in diesem Bildschirm angezeigten Einstellungen auf die zuletzt gespeicherten Werte zurückzusetzen, klicken Sie auf **Zurücksetzen**.
9. Um die Einstellungen auf dieser Registerkarte auf die werkseitigen Standardwerte zurückzusetzen, klicken Sie auf **Standardwerte**.



Die Schaltfläche **Neustart** steht in diesem Bildschirm zur Verfügung. Weitere Informationen finden Sie unter ”Neustart”, auf Seite 103.

Die folgende Tabelle enthält ausführliche Informationen zum Einstellen des QoS-Leistungsmerkmals.

Klassifizierung				**Modus**
Unterstützung von WMM-Priorität	**Unterstützung von Legacy-Priorität**	**WMM- oder 802.11e-Client**	**Nicht-WMM-/Nicht-802.11e-Client**	
Deaktivieren	Deaktivieren	Nein	Nein	Alle Clients werden als Nicht-QoS-aktiviert verbunden. Alle Tx-Frames werden AC_BE zugewiesen und ohne einen IEEE 802.11 QoS-Steuerungsheader gesendet.
Aktivieren	Deaktivieren	Ja	Nein	Der WMM- oder 802.11e-Client wird als QoS-aktiviert verbunden. Jeder Tx-Frame wird korrekt klassifiziert und der entsprechenden Warteschlange zugewiesen. Der Frame wird mit QoS-Steuerungsheader gesendet. Für den Nicht-WMM-/Nicht-802.11e-Client wird der Tx-Frame nicht klassifiziert und über AC_BE ohne einen QoS-Steuerungsheader gesendet.
Deaktivieren	Aktivieren	n. zutr.	Ja	Alle Clients werden als Nicht-QoS-aktiviert verbunden. Jeder Tx-Frame wird korrekt klassifiziert und der entsprechenden Warteschlange zugewiesen. Der Frame wird ohne einen QoS-Steuerungsheader gesendet.
Aktivieren	Aktivieren	Ja	Ja	Der WMM- oder 802.11e-Client wird als QoS-aktiviert verbunden. Jeder Tx-Frame wird korrekt klassifiziert und der entsprechenden Warteschlange zugewiesen. Der Frame wird abhängig davon, ob der Client als QoS-aktiviert verbunden ist oder nicht, mit/ohne QoS-Steuerungsheader gesendet.

Tabelle 13 Einstellen der QoS-Klassifizierung

6.4 Verwalten der Konfiguration

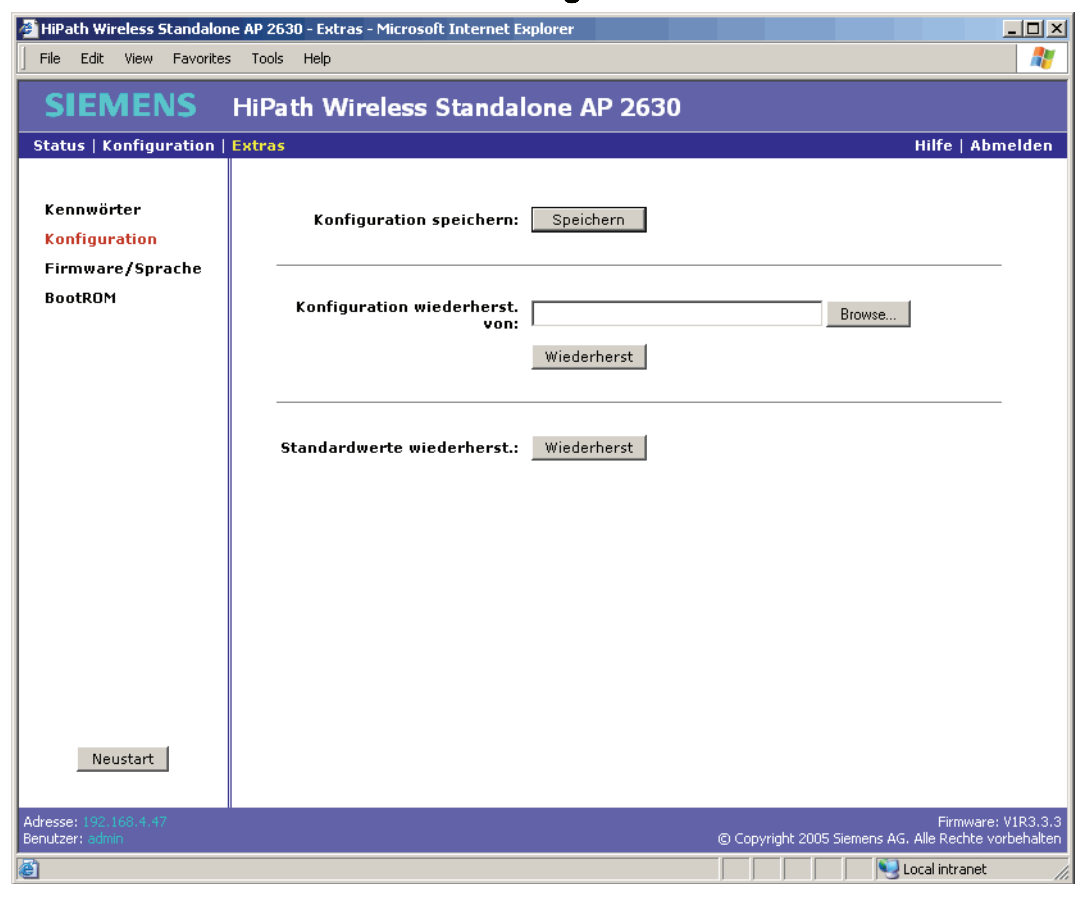
Der Standalone Access Point ermöglicht Ihnen, Standalone Access Point-Konfigurationen zu speichern und zu einem späteren Zeitpunkt wiederherzustellen. Sie können auch die werkseitigen Standardeinstellungen wiederherstellen.

6.4.1 Speichern der Konfiguration

Verwenden Sie den Bildschirm **Konfiguration**, um eine Standalone Access Point-Konfiguration in einer Datei zu speichern.

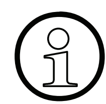
So speichern Sie die Konfiguration:

1. Klicken Sie in der Menüleiste auf **Extras**.
2. Klicken Sie im linken Fenster auf **Konfiguration**.



3. Klicken Sie im Bereich **Konfiguration speichern** auf **Speichern**, um die aktuelle Konfiguration zu speichern. Das Dialogfeld **Dateidownload** wird angezeigt.
4. Klicken Sie im Dialogfeld **Dateidownload** auf **Speichern**.

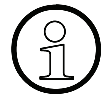
5. Geben Sie im Dialogfeld **Speichern unter** einen Ort an, an dem die Datei gespeichert werden soll.
6. Geben Sie im Feld **Dateiname** den Namen für die Konfigurationsdatei (.cfg) ein.
7. Um die Konfigurationsdatei im gewählten Verzeichnis zu speichern, klicken Sie auf **Speichern**.



Die Schaltfläche **Neustart** steht in diesem Bildschirm zur Verfügung. Weitere Informationen finden Sie unter ”Neustart”, auf Seite 103.

6.4.2 Wiederherstellen der Konfiguration

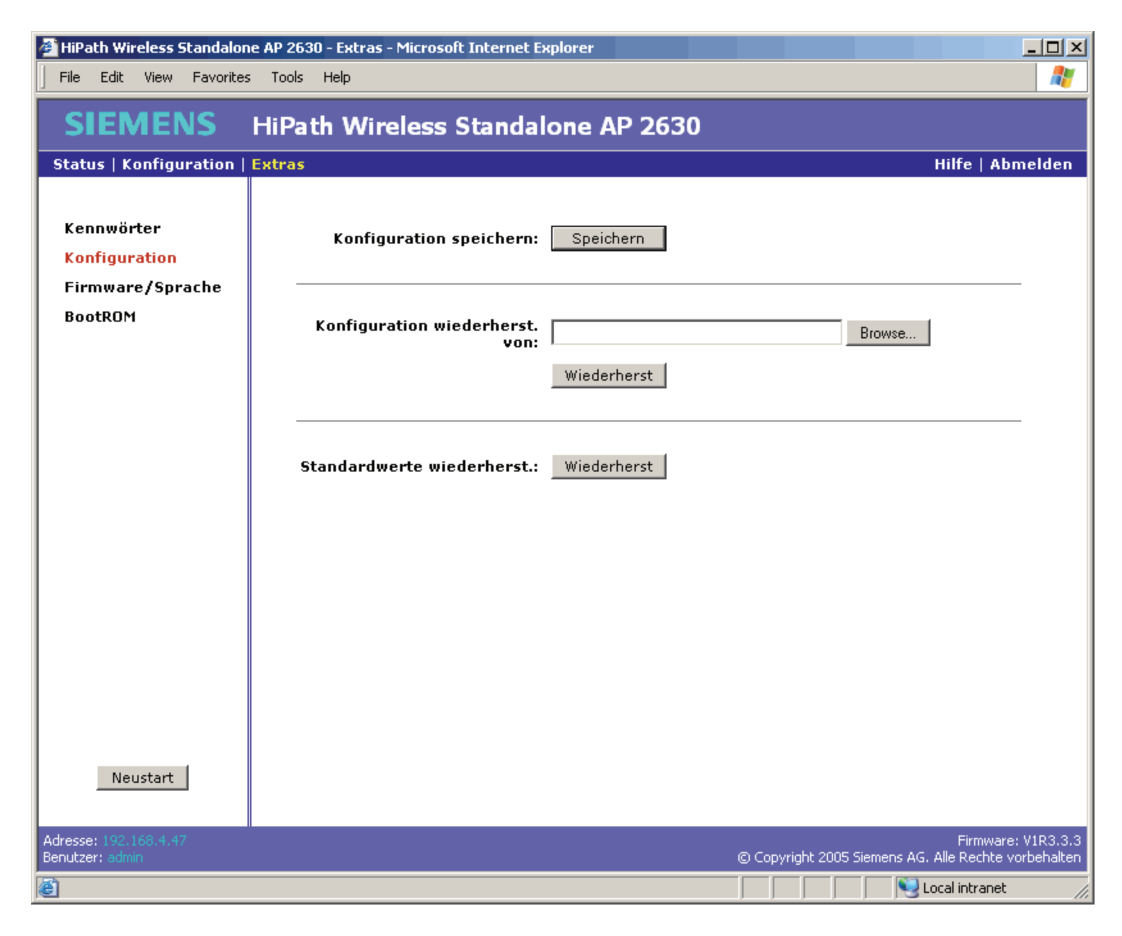
Verwenden Sie den Bildschirm **Konfiguration**, um eine Standalone Access Point-Konfiguration aus einer Datei wiederherzustellen.



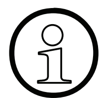
Wenn die Konfiguration wiederhergestellt wird, setzt die Software zunächst alle Konfigurationsparameter auf die werkseitigen Standardeinstellungen zurück. Anschließend wendet die Software die Befehle in der angegebenen Konfigurationsdatei an.

So stellen Sie eine Konfiguration wieder her:

1. Klicken Sie in der Menüleiste auf **Extras**.
2. Klicken Sie im linken Fenster auf **Konfiguration**.



3. Klicken Sie im Bereich **Konfiguration wiederherst. von** auf **Durchsuchen**, um zur entsprechenden Konfigurationsdatei zu navigieren.
4. Wählen Sie die Datei aus, die heruntergeladen werden soll, und klicken Sie im Dialogfeld **Datei auswählen** auf **Öffnen**. Der Verzeichnispfad wird im Feld **Konfiguration wiederherst. von** angezeigt.
5. Klicken Sie im Bereich **Konfiguration wiederherst. von** auf **Wiederherst**.



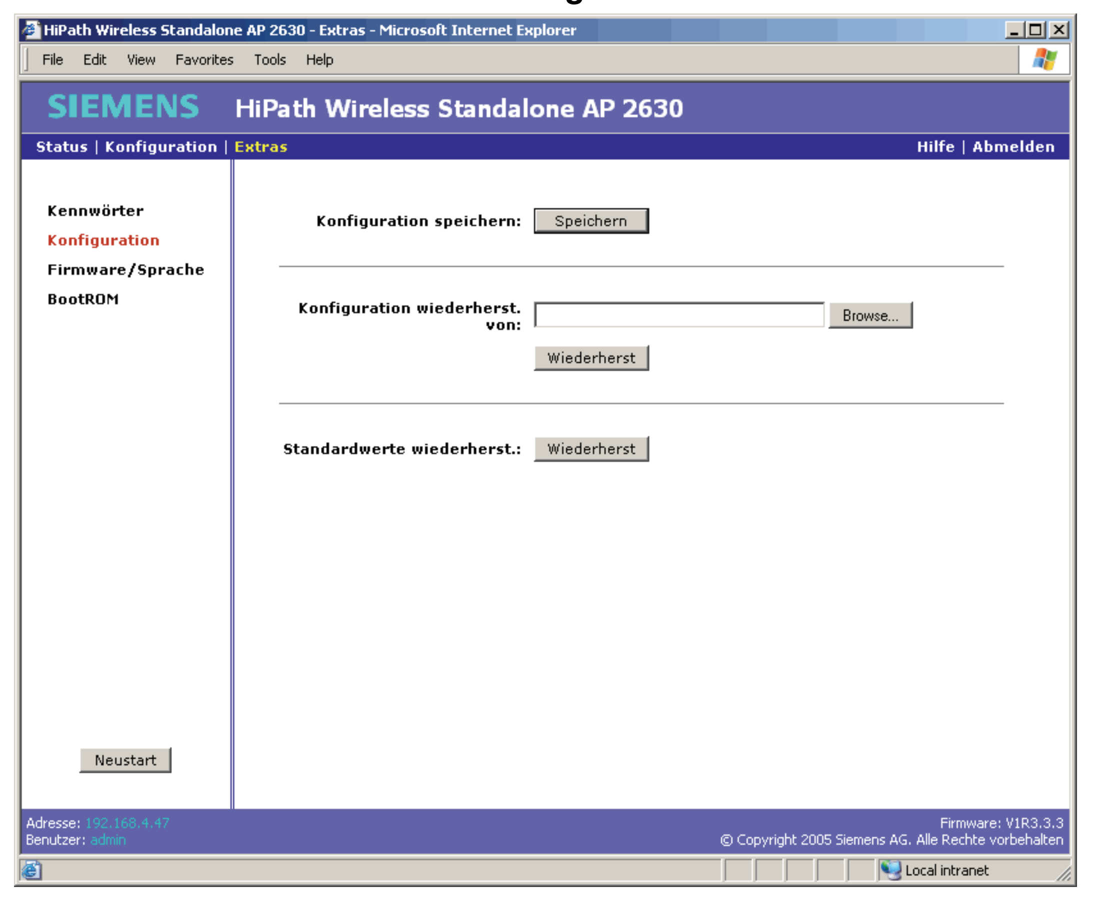
Der Standalone Access Point wird automatisch **neu gestartet**, nachdem eine Konfiguration wiederhergestellt wurde. Weitere Informationen finden Sie unter ”Neustart”, auf Seite 103.

6.4.3 Wiederherstellen der werkseitigen Standardeinstellungen

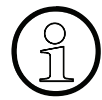
Verwenden Sie den Bildschirm **Konfiguration**, um alle Standalone Access Point-Einstellungen auf die Standardwerte zurückzusetzen.

So stellen Sie alle Standardeinstellungen wieder her:

1. Klicken Sie in der Menüleiste auf **Extras**.
2. Klicken Sie im linken Fenster auf **Konfiguration**.



3. Klicken Sie im Abschnitt **Standardwerte wiederherst.** auf **Wiederherstellen**.



Der Standalone Access Point wird automatisch neu gestartet, nachdem alle werkseitigen Standardeinstellungen wiederhergestellt wurden. Weitere Informationen finden Sie unter ”Neustart”, auf Seite 103.

6.4.4 Aktualisieren des BootROM

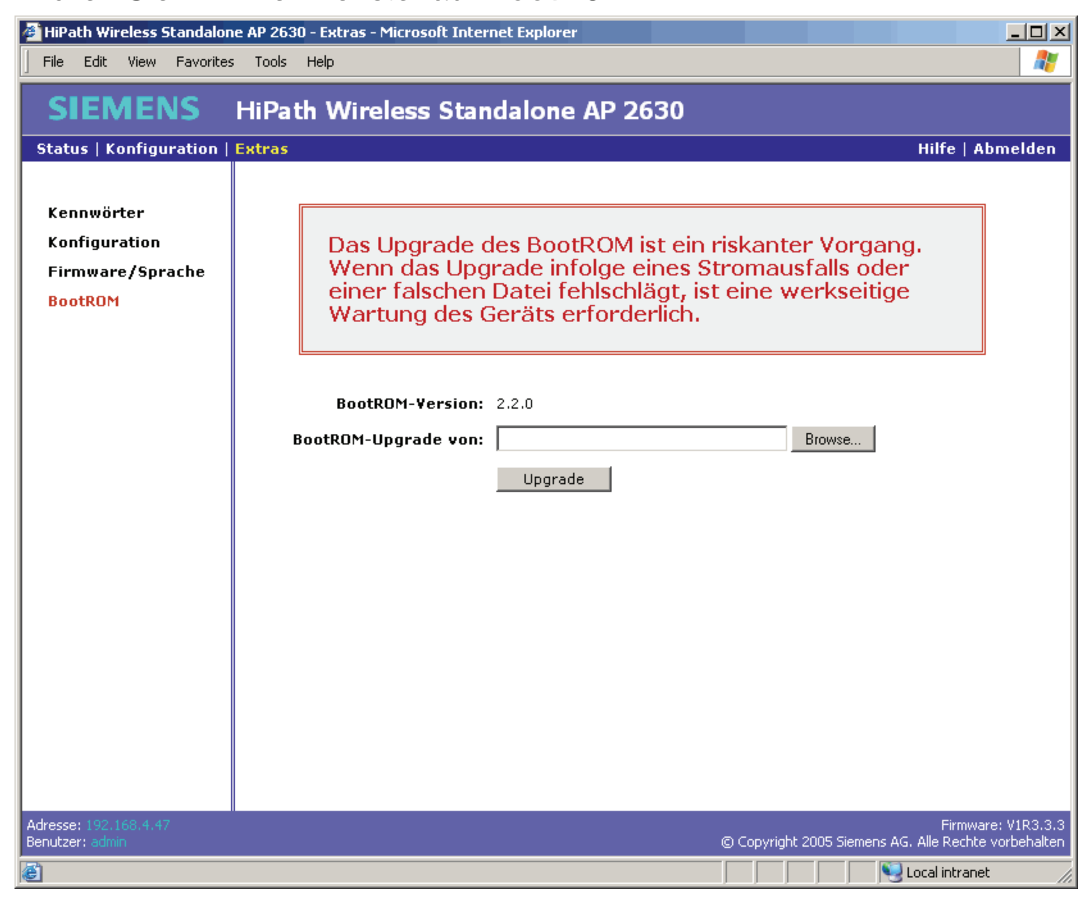
Verwenden Sie den Bildschirm **BootROM**, um den BootROM zu aktualisieren. Sie können auf dem Host, der den Webclient ausführt, einen Pfad eingeben oder auswählen, von dem der neue BootROM heruntergeladen werden soll. Der neue BootROM wird über den bestehenden BootROM installiert.



Das Aktualisieren des BootROM ist ein überaus riskanter Vorgang. Wenn die Aktualisierung aus irgendeinem Grund fehlschlägt, zum Beispiel wegen eines Stromausfalls oder einer falschen Datei, ist eine werkseitige Wartung des Geräts erforderlich.

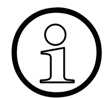
So aktualisieren Sie den BootROM:

1. Klicken Sie in der Menüleiste auf **Extras**.
2. Klicken Sie im linken Fenster auf **BootROM**.



3. Klicken Sie im Bereich **BootROM-Upgrade von** auf **Durchsuchen**, um zur entsprechenden Datei zu navigieren.

4. Wählen Sie die Datei aus, die heruntergeladen werden soll, und klicken Sie im Dialogfeld **Datei auswählen** auf **Öffnen**. Der Verzeichnispfad wird im Feld **BootROM-Upgrade von** angezeigt.
5. Klicken Sie auf **Upgrade**. Die ausgewählte Datei wird heruntergeladen.



Der Standalone Access Point wird nach dem Download des neuen BootROM automatisch mit der neuen BootROM-Version neu gestartet. Weitere Informationen finden Sie unter ”Neustart”, auf Seite 103.

7 Problembehandlung beim Standalone Access Point

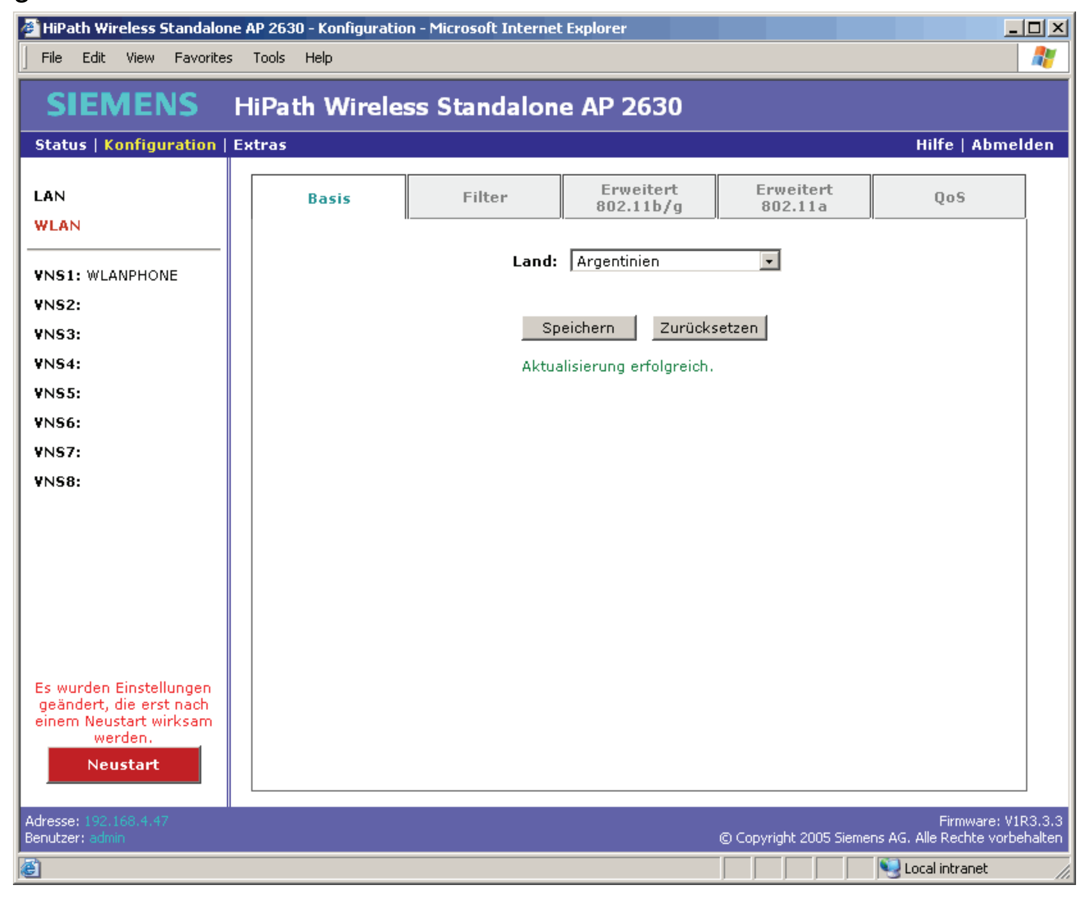
7.1 Neustart

Sie können auf die Schaltfläche **Neustart** klicken, um den Standalone Access Point neu zu starten. Wenn die Konfiguration geändert wurde und ein Neustart erforderlich ist, ändert sich die Farbe der Schaltfläche **Neustart** von grau zu rot und der folgende Text wird angezeigt:

Es wurden Einstellungen geändert, die erst nach einem Neustart wirksam werden.

So starten Sie den Standalone Access Point neu:

1. Klicken Sie im linken Fenster auf **Neustart**. Der Standalone Access Point wird neu gestartet.



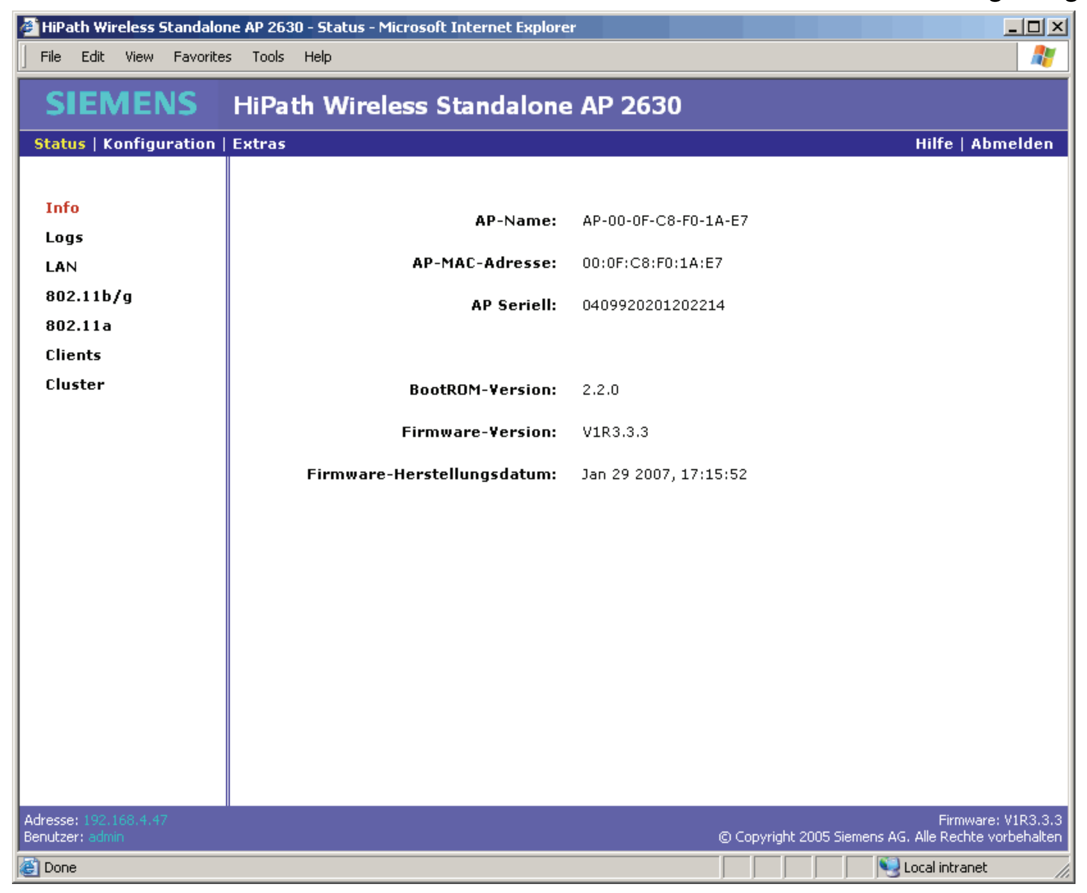
7.2 Anzeigen von Systemstatus-Informationen

Verwenden Sie den Bildschirm **Info**, um Informationen zum Systemstatus des Standalone Access Point anzuzeigen. Der Bildschirm zeigt Folgendes an:

- Name des Access Point
- MAC-Adresse des Access Point
- Seriennummer des Access Point
- BootROM-Version
- Firmware-Version
- Firmware Build-Datum

So zeigen Sie Informationen zum Systemstatus an:

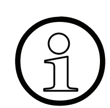
Klicken Sie in der Menüleiste auf **Status**. Der Bildschirm **Info** wird angezeigt.



7.3 Anzeigen von Protokollstatus-Informationen

Verwenden Sie den Bildschirm **Protokolle**, um Informationen zum Protokollstatus des Standalone Access Point anzuzeigen. Der Bildschirm zeigt den Inhalt der Flash-basierten Protokolldatei in einfach lesbarem Format an. Jeder Protokolleintrag wird in einer separaten Zeile angezeigt. Sie können folgende Protokollstatus-Informationen anzeigen:

- Eine eindeutige Sitzungsnummer, die sich bei jedem Neustart des Standalone Access Point erhöht. Diese Nummer wird bei 255 zurückgestellt.
- Die Zeitmarke in der Sitzung, angezeigt in Tagen, Stunden, Minuten und Sekunden seit dem Start der Sitzung.
- Einen Ereigniscode.
- Eine Protokollmeldung-Ereignisbeschreibung, die Text und optionale Parameter enthält, zum Beispiel MAC- und IP-Adressen.

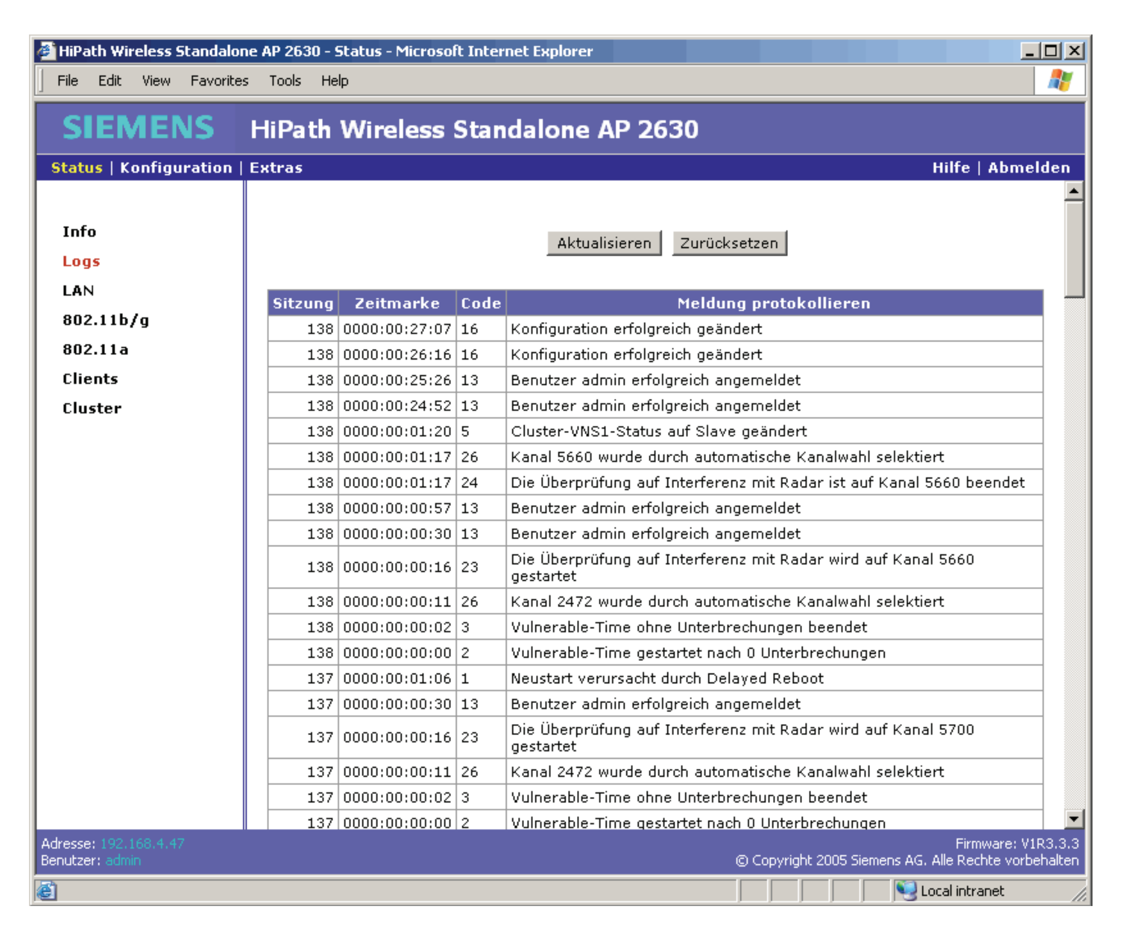


Das Protokoll zeigt nur die letzten 50 Ereignisse.

Weitere Informationen finden Sie im Anhang A, “Anhang: Protokollcodes und -meldungen”.

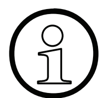
So zeigen Sie Informationen zum Protokollstatus an:

1. Klicken Sie in der Menüleiste auf **Status**.
2. Klicken Sie im linken Fenster auf **Protokolle**.



3. Zum Aktualisieren der angezeigten Protokolldaten auf die aktuellsten Daten klicken Sie auf **Aktualisieren**.

4. Zum Löschen aller Einträge aus dem Protokoll klicken Sie auf **Zurücksetzen.** Diese Schaltfläche ist für Benutzer mit Nur-Lese-Berechtigung deaktiviert.



Beim Zurücksetzen der Hardware oder Software auf die Standardeinstellungen wird das Protokoll nicht gelöscht. Beide Ereignisse werden im Protokoll mittels unterschiedlicher Codes dokumentiert. Weitere Informationen finden Sie im Kapitel 3.1 "Zurücksetzen auf werkseitige Standardeinstellungen" auf Seite 15 oder im Kapitel 5.2.3 "Wiederherstellen der werkseitigen Standardeinstellungen" auf Seite 41.

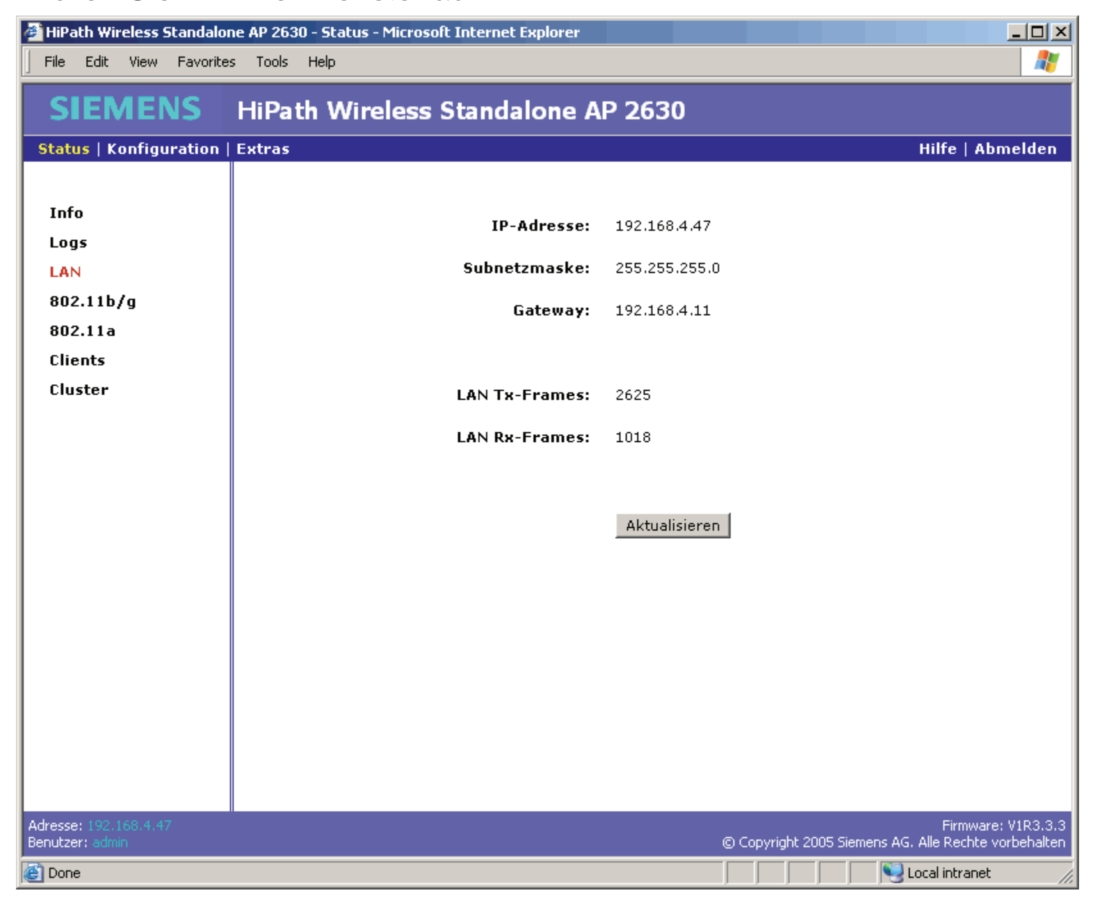
7.4 Anzeigen von LAN-Status-Informationen

Verwenden Sie den Bildschirm **LAN**, um Informationen zum LAN-Status des Standalone Access Point anzuzeigen. Der Bildschirm zeigt Folgendes an:

- IP-Adresse
- Subnetzmaske
- Gateway
- Anzahl der LAN-Tx-Frames
- Anzahl der LAN-Rx-Frames

So zeigen Sie Informationen zum LAN-Status an:

1. Klicken Sie in der Menüleiste auf **Status**.
2. Klicken Sie im linken Fenster auf **LAN**.



3. Zum Aktualisieren der angezeigten LAN-Daten auf die aktuellsten Daten klicken Sie auf **Aktualisieren**.

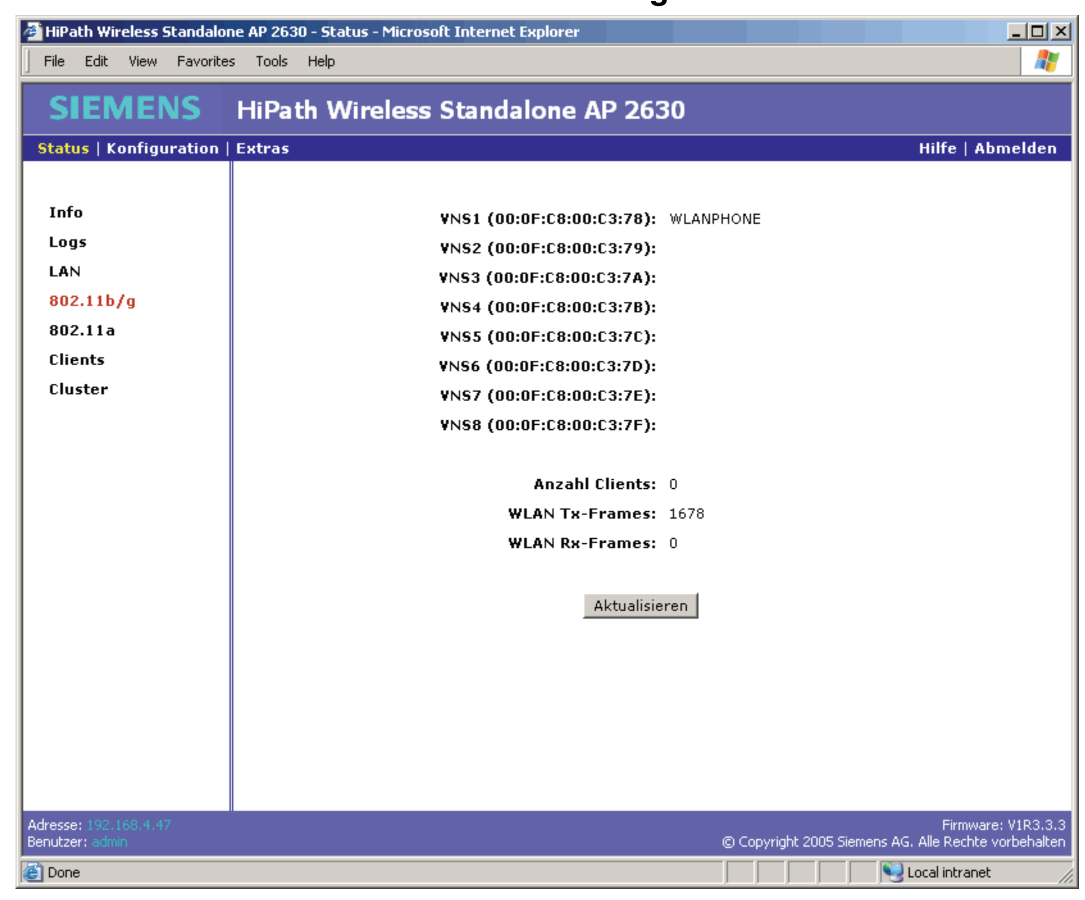
7.5 Anzeigen von 802.11b/g-Statusinformationen

Verwenden Sie den Bildschirm **802.11b/g**, um Informationen zum 802.11b/g-Status des Standalone Access Point anzuzeigen. Der Bildschirm zeigt Folgendes an:

- Funkstatus des VNS. Beachten Sie, dass der Funk immer deaktiviert ist, wenn der Standalone Access Point nicht im Cluster ist. BSSID - Eine 48-Bit-Kennung, die ein bestimmtes BSS (Basic Service Set) identifiziert, wird immer angezeigt. Für jeden aktivierten VNS wird der SSID-Name angezeigt.
- Name und Status des VNS (SSID)
- Anzahl der derzeit mit diesem Standalone Access Point auf diesem Funkmodul verbundenen Clients
- Anzahl der drahtlosen Tx-Frames
- Anzahl der drahtlosen Rx-Frames

So zeigen Sie Informationen zum 802.11b/g-Status an:

1. Klicken Sie in der Menüleiste auf **Status**.
2. Klicken Sie im linken Teilfenster auf **802.11b/g**.



3. Zum Aktualisieren der angezeigten Daten auf die aktuellsten Daten klicken Sie auf **Aktualisieren**.

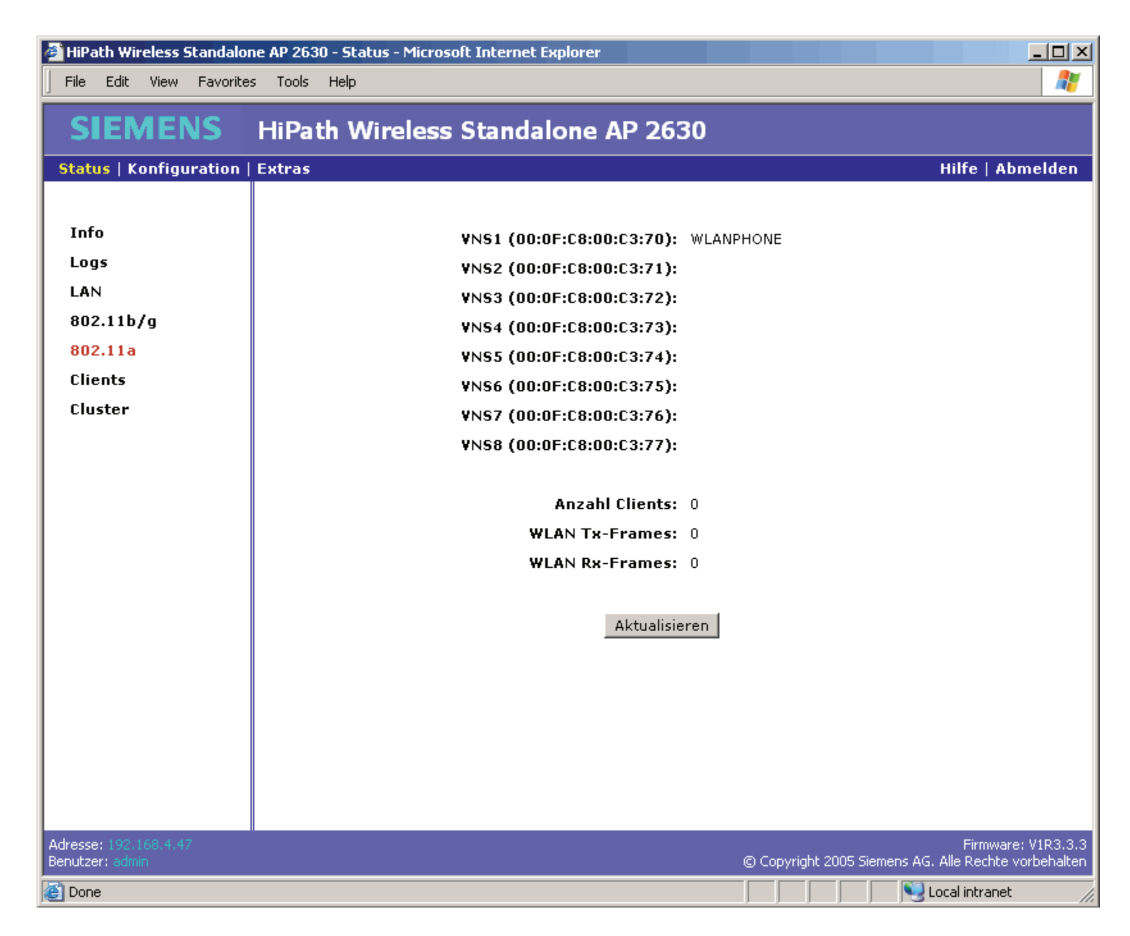
7.6 Anzeigen von 802.11a-Statusinformationen

Verwenden Sie den Bildschirm **802.11a**, um Informationen zum 802.11a-Status des Standalone Access Point anzuzeigen. Der Bildschirm zeigt Folgendes an:

- Funkstatus des VNS. Beachten Sie, dass der Funk immer deaktiviert ist, wenn der Standalone Access Point nicht im Cluster ist. BSSID - Eine 48-Bit-Kennung, die ein bestimmtes BSS (Basic Service Set) identifiziert, wird immer angezeigt. Für jeden aktivierten VNS wird der SSID-Name angezeigt.
- Name und Status des VNS (SSID)
- Anzahl der derzeit mit diesem Standalone Access Point auf diesem Funkmodul verbundenen Clients
- Anzahl der drahtlosen Tx-Frames
- Anzahl der drahtlosen Rx-Frames

So zeigen Sie Informationen zum 802.11a-Status an:

1. Klicken Sie in der Menüleiste auf **Status**.
2. Klicken Sie im linken Teilfenster auf **802.11a**.



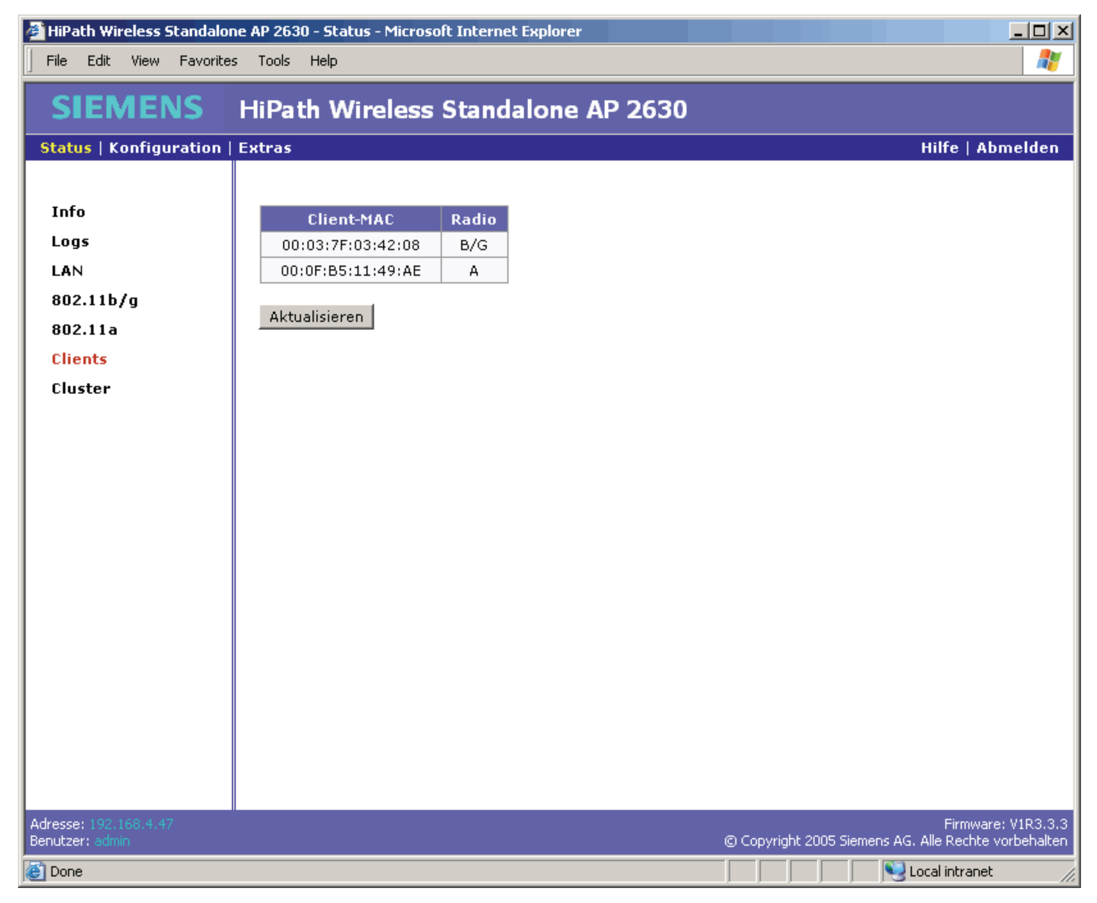
3. Zum Aktualisieren der angezeigten Daten auf die aktuellsten Daten klicken Sie auf **Aktualisieren**.

7.7 Anzeigen von Informationen zum Client-Status

Verwenden Sie den Bildschirm **Clients**, um Informationen zum Client-Status des Standalone Access Point anzuzeigen. Der Bildschirm zeigt die MAC-Adresse des Client und das verwendete Funkmodul an.

So zeigen Sie Informationen zum Client-Status an:

1. Klicken Sie in der Menüleiste auf **Status**.
2. Klicken Sie im linken Fenster auf **Clients**.



3. Zum Aktualisieren der angezeigten Client-Daten auf die aktuellsten Daten klicken Sie auf **Aktualisieren**.

7.8 Anzeigen von Informationen zum Cluster-Status

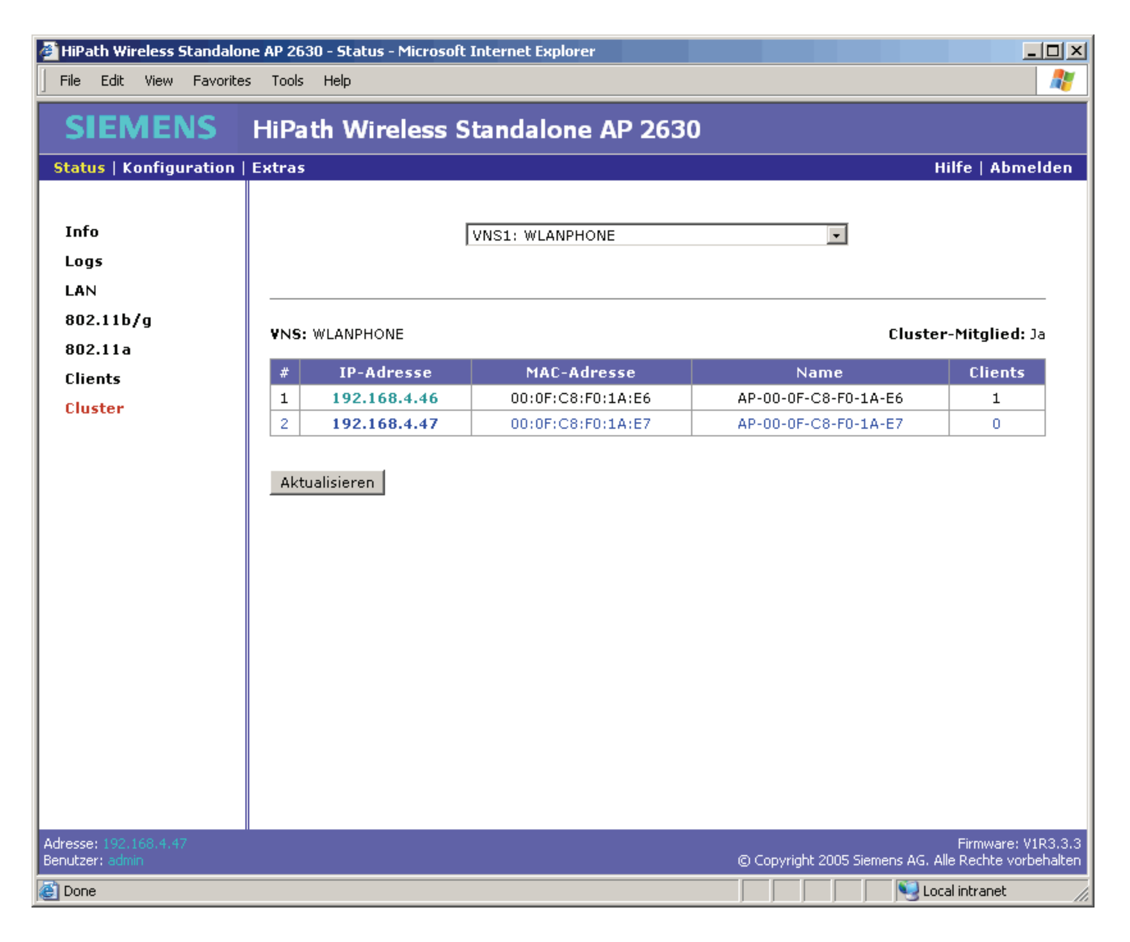
Verwenden Sie den Bildschirm **Cluster**, um Cluster-Informationen für den Standalone Access Point anzuzeigen. Auf dem Bildschirm wird die Liste der Standalone Access Points angezeigt, die derzeit im Cluster registriert sind. Für jeden aktivierten VNS wird der SSID-Name in der Dropdown-Liste angezeigt. Jeder Standalone Access Point wird mit folgenden Informationen angezeigt:

- Rang in dem Cluster
- IP-Adresse
- MAC-Adresse
- Name
- Anzahl der derzeit mit dem Standalone Access Point verbundenen Clients

Die Standalone Access Points sind in ihrer Rangfolge aufgelistet. Weitere Informationen finden Sie unter ”Info zu Clustering”, auf Seite 48. Wenn der aktuelle Standalone Access Point nicht Teil des Clusters ist, wird der Cluster auf dem Bildschirm ohne den aktuellen Standalone Access Point angezeigt.

So zeigen Sie Informationen zum Cluster-Status an:

1. Klicken Sie in der Menüleiste auf **Status**.
2. Klicken Sie im linken Fenster auf **Cluster**.



3. Klicken Sie in der Dropdown-Liste **VNS** auf die SSID für den VNS, den Sie anzeigen möchten.

4. Zum Aktualisieren der angezeigten Cluster-Daten auf die aktuellsten Daten klicken Sie auf **Aktualisieren**.

8 Konvertieren von Access Points

Sie haben nun die Möglichkeit, Access Points zu konvertieren. Folgende Access Points können konvertiert werden:

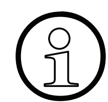
- Standalone Access Points 2630/2640 in Access Points 2610/2620
- Access Points 2610/2620 in Standalone Access Points 2630/2640

8.1 Konvertieren eines Standalone Access Point 2630/2640 in einen Access Point 2610/2620

Um einen Standalone Access Point 2630/2640 zu konvertieren, müssen Sie den Standalone Access Point Build V1R3.3.4 oder höher verwenden. Wenn die Access Point 2610/2620-Abbilddatei nicht bereits auf Ihrem lokalen Netzwerk verfügbar ist, wenden Sie sich an Ihren Netzwerkadministrator.

So konvertieren Sie einen Standalone Access Point 2630/2640:

1. Klicken Sie in der Menüleiste auf **Extras**.
2. Klicken Sie im linken Fenster auf **Firmware/Sprache**.
3. Klicken Sie im Bereich **Firmware downloaden von** auf **Durchsuchen**, um zur AP2610/2620-Abbilddatei zu navigieren.
4. Wählen Sie die Abbilddatei aus, und klicken Sie im Dialogfeld **Datei auswählen** auf **Öffnen**. Der Verzeichnispfad wird im Feld **Firmware downloaden von** angezeigt.
5. Klicken Sie auf **Download und Neustart**. Die ausgewählte Datei wird heruntergeladen, und der Standalone Access Point wird neu gestartet. Nach dem Neustart wird der Standalone Access Point in den Access Point 2610/2620 konvertiert, und die Konfiguration wird auf die Standardkonfiguration für den Access Point 2610/2620 zurückgesetzt.



Die Konvertierung wirkt sich nicht auf den Modellnamen des Access Point aus; der Modellname für den Access Point bleibt unverändert.

8.2 Konvertieren eines Access Point 2610/2620 in einen Standalone Access Point 2630/2640

Zum Konvertieren eines Access Point 2610/2620 ist Folgendes erforderlich:

- Access Point 2610/2620 Build V4R1.1.11 oder höher
- Zugriff auf den HiPath Wireless Assistant, mit Build V4R1.1.11 oder höher

- Der Access Point 2610/2620 muss mit dem HiPath Wireless Controller verbunden sein.

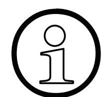
Weitere Informationen finden Sie im *HiPath Wireless Controller, Access Points und Convergence Software Benutzerhandbuch*.

So konvertieren Sie einen Access Point 2610/2620:

1. Melden Sie sich bei HiPath Wireless Assistant an.
2. Klicken Sie im Hauptmenü auf **Wireless AP Configuration**. Der Bildschirm **HiPath Wireless AP** wird angezeigt.
3. Klicken Sie im linken Fenster auf **AP Maintenance**. Die Registerkarte **AP Software Maintenance** wird angezeigt.
4. Laden Sie die Access Point 2630/2640-Abbilddatei von einem FTP-Server herunter. Geben Sie in der Liste **Download AP Images** Folgendes ein:
    - **FTP Server** – Die IP-Adresse des FTP-Servers, von dem die Abbilddatei abgerufen werden soll.
    - **User ID** – Die Benutzer-ID, die der Controller verwenden soll, wenn er versucht, sich beim FTP-Server anzumelden.
    - **Password** – Das zu der Benutzer-ID gehörende Kennwort.
    - **Confirm** – Erneute Eingabe des Kennworts zur Bestätigung der korrekten Eingabe.
    - **Directory** – Das Verzeichnis auf dem Server, in dem die abzurufende Abbilddatei gespeichert ist.
    - **Filename** – Der Name der abzurufenden Abbilddatei.
    - **Platform** – Der AP-Hardwaretyp, auf den sich die Abbilddatei bezieht.
5. Klicken Sie auf **Download**. Das neue Softwareabbild wird auf den HiPath Wireless Controller heruntergeladen.
6. Klicken Sie auf die Registerkarte **Controlled Upgrade**.
7. Klicken Sie in der Dropdown-Liste in **Step 1** auf den Access Point-Hardwaretyp, auf den sich die Abbilddatei bezieht.
8. Klicken Sie in der Dropdown-Liste in **Step 2** auf das Access Point 2630/2640-Abbild, das Sie auf den HiPath Wireless Controller heruntergeladen haben.
9. Wählen Sie in der Tabelle in **Step 3** die Access Points aus, die Sie konvertieren möchten, und klicken Sie auf **Apply AP image version**.
10. Klicken Sie auf **Upgrade Now**.

11. Das Access Point-Abbild wird angewendet, und die ausgewählten Access Points werden neu gestartet. Nach dem Neustart werden die Access Points in den Standalone Access Point konvertiert, und die Konfiguration wird auf die Standardkonfiguration für den Standalone Access Point zurückgesetzt.

12. Nach abgeschlossener Konvertierung klicken Sie in der Dropdown-Liste in **Step 2** auf **No upgrade** und anschließend auf **Apply AP image version**. Dieser abschließende Schritt stellt sicher, dass die konvertierten Access Points nicht fortlaufend in Standalone Access Points 2630/2640 konvertiert werden, wenn sie zu einem späteren Zeitpunkt als Access Points 2610/2620 mit dem HiPath Wireless Controller verbunden werden.



Die Konvertierung wirkt sich nicht auf den Modellnamen des Access Point aus; der Modellname für den Access Point bleibt unverändert.

9 Glossar: Netzwerk-Begriffe und -Abkürzungen

Begriff	Definition
AAA	Authentication, Authorization, Accounting. Ein System in IP-basierten Netzwerken zur Kontrolle der Computerressourcen, auf die Benutzer zugreifen können, und zur Überwachung und Dokumentation der Aktivitäten von Benutzern in einem Netzwerk.
AC	Access Class (Zugangsklasse)
AC_BE	Access Class - Best Effort (Best-Effort-Zugangsklasse)
Access Point (AP)	Der Standalone Access Point ist ein WLAN-Access Point (IEEE 802.11), der mit einer speziellen Software ausgerüstet ist, die es ihm ermöglicht, nur mit einem Access Point zu kommunizieren. (Ein Thin Access Point verwaltet die Funkfrequenz-Kommunikation, benötigt aber einen Controller, um WLAN-Elemente wie zum Beispiel Authentifizierung zu nutzen.) Der Standalone Access Point bietet auch lokale Verarbeitungsfunktionen, zum Beispiel Verschlüsselung. Der Standalone Access Point ist ein Dual-Band Access Point mit 802.11a+b/g-Funk.
Ad-hoc-Modus	Eine 802.11-basierte Netzwerkstruktur, in der Geräte oder Stationen ohne Verwendung eines Access Point (AP) direkt miteinander kommunizieren. (Vergleiche Infrastruktur-Modus)
AES	Advanced Encryption Standard (AES) Ein Verschlüsselungsalgorithmus, der gleichzeitig auf mehreren Netzwerkschichten funktioniert. AES bedient sich der blockweisen Verschlüsselung, um Daten in Blöcken fester Größe mit 128 Bit zu verschlüsseln. AES wurde vom National Institute of Standards and Technology (NIST) entwickelt. AES ist eine Datenschutz-Transformation (Privacy Transform) für IPSec und Internet Key Exchange (IKE). AES hat eine variable Schlüssellänge – der Algorithmus kann einen 128-Bit-Schlüssel (der Standard), einen 192-Bit-Schlüssel oder einen 256-Bit-Schlüssel definieren. Für die WPA2/802.11i-Implementierung von AES wird eine Schlüssellänge von 128 Bit verwendet. Die AES-Verschlüsselung umfasst vier Stadien, die zusammen eine Runde bilden. Jede Runde wird dann abhängig von der Bit-Schlüsselgröße 10-, 12- oder 14-mal wiederholt. Für die WPA2/802.11i-Implementierung von AES wird jede Runde 10-mal wiederholt.

Begriff	Definition
AES-CCMP	AES verwendet das Counter-Modus/CBC-MAC-Protokoll (CCMP). CCM ist ein neuer Betriebsmodus für eine blockweise Verschlüsselung, der die Verwendung eines einzigen Schlüssels für Verschlüsselung sowie Authentifizierung ermöglicht. Die beiden in CCM verwendeten zugrunde liegenden Modi sind Counter-Modus (CTR) für die Datenverschlüsselung und Cipher Block Chaining Message Authentication Code (CBC-MAC) zur Gewährleistung der Datenintegrität.
ARP	Address Resolution Protocol. Dieses Protokoll wird verwendet, um die physikalischen Adressen (zum Beispiel MAC-Adressen) von Hardwaregeräten in einer Netzwerkumgebung abzurufen. Ein Host ruft eine solche physikalische Adresse ab, indem er eine ARP-Anforderung rundsendet, die die IP-Adresse des Ziel-Hardwaregeräts enthält. Wenn die Anforderung ein Gerät mit dieser IP-Adresse findet, antwortet das Gerät mit seiner physikalischen Hardwareadresse.
BOF	Grafische Benutzeroberfläche
BSS	Basic Service Set. Eine drahtlose Topologie, die aus einem Access Point besteht, der mit einem drahtgebundenen Netzwerk und einem Satz von drahtlosen Geräten verbunden ist. Wird auch als Infrastruktur-Netzwerk bezeichnet. *Siehe auch* IBSS.
Datagramm	Ein Datagramm ist "eine in sich geschlossene, unabhängige Dateneinheit, die genügend Informationen transportiert, um vom Ursprungs- zum Zielcomputer übermittelt zu werden, ohne dass ein vorheriger Austausch zwischen dem Ursprungs- und Zielcomputer und dem transportierenden Netzwerk erforderlich ist." (RFC1594). Für den Begriff Datagramm hat sich allgemein der Begriff Paket durchgesetzt. Datagramme oder Pakete sind die Nachrichteneinheiten, mit denen das Internetprotokoll befasst ist und die über das Internet transportiert werden.

Begriff	Definition
DHCP	Dynamic Host Configuration Protocol. Ein Protokoll für die Zuweisung dynamischer IP-Adressen an Geräte in einem Netzwerk. Bei der dynamischen Adressierung kann ein Gerät bei jeder Verbindungsherstellung zum Netzwerk eine andere IP-Adresse haben. Bei einigen Systemen kann sich die IP-Adresse des Geräts sogar ändern, während es verbunden ist. DHCP unterstützt auch eine Mischung aus statischen und dynamischen IP-Adressen. DHCP besteht aus zwei Komponenten: einem Protokoll für die Übermittlung Host-spezifischer Konfigurationsparameter von einem DHCP-Server zu einem Host und einem Mechanismus für die Zuweisung von Netzwerkadressen an Hosts. (IETF RFC1531.) Option 78 gibt den Standort von einem oder mehreren SLP Directory Agents an. Option 79 gibt die Liste der Bereiche an, für deren Verwendung ein SLP Agent konfiguriert ist. (RFC2610 - DHCP Options for Service Location Protocol.)
DSSS	Direct-Sequence Spread Spectrum. Eine bei WLAN-Übertragungen verwendete Übermittlungstechnik, bei der ein Datensignal an der sendenden Station mit einer Bitfolge mit höherer Datenrate kombiniert wird, dem sogenannten Chipping Code, der eine Spreizung der Nutzdaten in einem bestimmten Verhältnis bewirkt. Der Chipping Code ist ein redundantes Bitmuster für jedes übertragene Bit, wodurch die Resistenz des Signals gegen Störungen erhöht wird. Wenn ein oder mehrere Bits in dem Muster während der Übertragung beschädigt werden, können die Originaldaten aufgrund der Redundanz der Übertragung wiederhergestellt werden. (Vergleiche FHSS)
DTIM	Delivery Traffic Indication Message (im 802.11-Standard)

Begriff	Definition
EAP-TLS EAP-TTLS	Extensible Authentication Protocol - Transport Layer Security (EAP-TLS). Ein allgemeines Authentifizierungsprotokoll, das mehrere Authentifizierungsmethoden unterstützt, zum Beispiel Token-Karten, Kerberos, Einmal-Kennwörter, Zertifikate, Authentifizierung mit öffentlichem Schlüssel und Smart Cards. IEEE 802.1x gibt an, wie EAP in LAN-Frames zu verkapseln ist. Bei drahtloser Kommunikation mit EAP fordert ein Benutzer die Verbindung zu einem WLAN über einen Access Point an, der dann die Identität des Benutzers anfordert und diese Identität an einen Authentifizierungsserver, wie zum Beispiel RADIUS, übermittelt. Der Server fordert den Access Point zur Bestätigung der Identität auf. Diese erhält der Access Point vom Benutzer und sendet sie anschließend zurück zum Server, um die Authentifizierung abzuschließen. EAP-TLS stellt zertifikatbasierte, gegenseitige Authentifizierung von Client und Netzwerk bereit. Es benötigt für die Authentifizierung clientseitige und serverseitige Zertifikate und kann zur dynamischen Generierung von benutzerbasierten und sitzungsbasierten WEP-Schlüsseln verwendet werden. EAP-TTLS (Tunneled Transport Layer Security) ist eine Erweiterung von EAP-TLS, um zertifikatbasierte, gegenseitige Authentifizierung von Client und Netzwerk über einen verschlüsselten Tunnel bereitzustellen und dynamische benutzer- und sitzungsbasierte WEP-Schlüssel zu generieren. Im Gegensatz zu EAP-TLS benötigt EAP-TTLS nur serverseitige Zertifikate. (*Siehe auch* PEAP)
ELA (OPSEC)	Event Logging API (Application Programming Interface) für OPSEC, ein Modul in Check Point, das es Drittanbieter-Anwendungen ermöglicht, Ereignisse im Check Point VPN-1/FireWall-1-Verwaltungssystem zu protokollieren.
ESS	Extended Service Set (ESS). Mehrere Basic Service Sets (BSSs) können verbunden werden, um ein logisches WLAN-Segment zu bilden, das als Extended Service Set (ESS) bezeichnet wird. Die SSID dient zum Identifizieren des ESS. (*Siehe* BSS und SSID.)
FHSS	Frequency-Hopping Spread Spectrum. Eine bei WLAN-Übertragungen verwendete Übermittlungstechnik, bei der das Datensignal mit einem Schmalband-Trägersignal moduliert wird, das in einer zufälligen aber vorhersehbaren Abfolge zeitbasiert in einem breiten Frequenzspektrum von Frequenz zu Frequenz wechselt. Durch diese Technik werden Übertragungsstörungen reduziert. Bei korrekter Synchronisierung wird ein einzelner logischer Kanal aufrechterhalten. (Vergleiche DSSS)

Begriff	Definition
Fit, Thin und Fat APs	Eine Thin AP-Architektur verwendet zwei Komponenten: einen Access Point, der praktisch ein verschlanktes Funksystem ist, und einen zentralen Verwaltungscontroller, der die anderen WLAN-Systemfunktionen ausführt. Drahtgebundene Netzwerk-Switches werden ebenfalls benötigt. Ein Fit AP, eine Variante des Thin AP, verwaltet Funkfrequenz und Verschlüsselung, während der zentrale Verwaltungscontroller, der die Identitäten und Standorte der drahtlosen Benutzer kennt, zuständig für sicheres Roaming, QoS und Benutzerauthentifizierung ist. Der zentrale Verwaltungscontroller ist außerdem zuständig für die AP-Konfiguration und -verwaltung. Bei einer Fat AP-Architektur ist die gesamte WLAN-Intelligenz im Access Point konzentriert. Der AP übernimmt die Funkfrequenz-Verwaltung, die Benutzerauthentifizierung, die Verschlüsselung der Kommunikation, das sichere Roaming, die WLAN-Verwaltung und, in einigen Fällen, auch das Netzwerk-Routing.
FTP	File Transfer Protocol
Gateway	Im Bereich der drahtlosen Kommunikation ein Access Point mit zusätzlichen Softwarefunktionen, um zum Beispiel NAT und DHCP bereitzustellen. Gateways können auch VPN-Unterstützung, Roaming, Firewalls, verschiedene Sicherheitsebenen etc. bereitstellen.
Host	(1) Ein Computer (der normalerweise Daten enthält), auf den ein Benutzer von einem Remote-Endgerät aus zugreift, das über Modems und Telefonleitungen verbunden ist. (2) Ein Computer, der mit einem TCP/IP-Netzwerk, zum Beispiel dem Internet, verbunden ist. Jeder Host hat eine eindeutige IP-Adresse.
HTTP	Hypertext Transfer Protocol ist ein Satz von Regeln für die Übertragung von Dateien (Text-, Grafik-, Audio-, Video- und andere Multimedia-Dateien) im World Wide Web. Die Nutzung von HTTP erfolgt über einen Webbrowser. HTTP ist ein Anwendungsprotokoll, das auf der TCP/IP-Protokollsammlung aufsetzt. (RFC2616: Hypertext Transfer Protocol -- HTTP/1.1)
IAPP	Inter-Access Point Protocol
IBSS	Independent Basic Service Set. *Siehe* BSS. Ein IBSS ist der 802.11-Begriff für ein Ad-hoc-Netzwerk. *Siehe* Ad-hoc-Netzwerk.
ICMP	Internet Control Message Protocol, eine durch RFC792 definierte Erweiterung zum Internetprotokoll (IP). ICMP unterstützt Pakete, die Fehler-, Steuerungs- und Informationsnachrichten enthalten. Beispielsweise nutzt der PING-Befehl ICMP, um eine Internetverbindung zu testen.
ICV	Integrity Check Value, ein 4-Byte-Code zur Integritätsprüfung, der beim Standard-WEP an die 802.11-Nachricht angehängt wird. Beim erweiterten WPA wird direkt vor dem ICV ein 8-Byte-MIC eingefügt. (*Siehe* WPA und MIC)

Begriff	Definition
IE	Internet Explorer.
IEEE	Institute of Electrical and Electronics Engineers, ein US-Verband von Ingenieuren und Technikern, die an der Definition von Standards beteiligt sind.
IETF	Internet Engineering Task Force, die wichtigste mit Standardisierungen für das Internet befasste Organisation.
Infrastruktur-Modus	Eine 802.11-basierte Netzwerkstruktur, in der Geräte über einen Access Point (AP) miteinander kommunizieren. Im Infrastruktur-Modus können drahtlose Geräte miteinander oder mit einem drahtgebundenen Netzwerk kommunizieren. (*Siehe* Ad-hoc-Modus und BSS.)
Internet- oder IP-Telefonie	Bei der IP- oder Internet-Telefonie erfolgt die Kommunikation, zum Beispiel Sprach-, Fax- oder Voice-Messaging-Verbindungen, nicht über das öffentliche Telefonnetz, sondern über das Internet. IP-Telefonie ist die bidirektionale Übertragung von Audiodaten über ein paketvermitteltes IP-Netzwerk (TCP/IP-Netzwerk). Ein Internet-Telefonanruf besteht aus zwei Schritten: (1) Umwandlung des analogen Sprachsignals in ein digitales Format, (2) Übersetzung des Signals in Internetprotokoll (IP)-Pakete zur Übertragung über das Internet. Am empfangenden Ende werden die Schritte umgekehrt. Die Sprachqualität bei Übertragungen über das öffentliche Internet schwankt erheblich. Um dies zu verbessern, werden Protokolle eingesetzt, die Quality of Service (QoS) unterstützen.
IP	Internetprotokoll bezeichnet die Methode oder das Protokoll, durch das Daten über das Internet von einem Computer zu einem anderen übertragen werden. Jeder Computer (Host) im Internet hat mindestens eine IP-Adresse, die ihn eindeutig identifiziert. Das Internetprotokoll definiert das Format der Pakete, auch als Datagramme bezeichnet, und das Adressierungsschema. Bei den meisten Netzwerken wird IP mit einem höherschichtigen Protokoll, dem Transmission Control Protocol (TCP) kombiniert, das eine virtuelle Verbindung zwischen einem Ursprung und einem Ziel einrichtet.
Isochrone Daten	Isochrone Daten sind Daten (zum Beispiel Sprache oder Video), die eine konstante Übertragungsrate erfordern, bei der die Daten in einem bestimmten Zeitrahmen übermittelt werden müssen. Beispielsweise erfordern Multimedia-Datenströme einen isochronen Transportmechanismus, um sicherzustellen, dass Daten praktisch zeitgleich mit ihrer Anzeige übermittelt und die Audio- mit den Videodaten synchronisiert werden. Vergleiche: asynchrone Prozesse, bei denen Datenströme in zufällige Intervalle unterteilt werden können, und synchrone Prozesse, bei denen Datenströme nur in bestimmten Intervallen übermittelt werden können.

Begriff	Definition
ISP	Internet Service Provider (Internetdienstanbieter).
IV	Initialisierungsvektor, ein Teil des Standardverfahrens der WEP-Verschlüsselung, bei dem ein gemeinsamer Kennwortschlüssel mit einem zufällig generierten 24-Bit-Initialisierungsvektor verkettet wird. WPA mit TKIP verwendet 48-Bit-IVs, eine Erweiterung, durch die ein Decodieren der Verschlüsselung erheblich erschwert wird. (*Siehe* WPA und TKIP)
Kollision	Wird verursacht, wenn zwei Ethernet-Pakete versuchen, das Medium gleichzeitig zu nutzen. Ethernet ist ein gemeinsam genutztes Medium, weshalb es Regeln für das Senden von Datenpaketen gibt, um Konflikte zu vermeiden und die Datenintegrität zu gewährleisten. Wenn zwei Knoten an unterschiedlichen Standorten versuchen, Daten zur gleichen Zeit zu senden, kommt es zur Kollision. Eine Methode zur Verringerung von Kollisionen in einem ausgelasteten Netzwerk besteht in der Segmentierung des Netzwerks durch Bridges oder Switches.
LAN	Local Area Network.
MAC	Media Access Control-Schicht. Eine von zwei Teilschichten, die die Sicherungsschicht des OSI-Modells bilden. Die MAC-Schicht ist zuständig für die Verschiebung von Datenpaketen zwischen zwei Netzwerkkarten (NICs) über einen gemeinsamen Kanal.
MAC-Adresse	Media Access Control-Adresse. Eine Hardwareadresse, die jeden Knoten in einem Netzwerk eindeutig identifiziert.
MIC	Message Integrity Check bzw. Code (MIC), auch als "Michael" bezeichnet, ein Bestandteil von WPA und TKIP. Der MIC ist ein zusätzlicher 8-Byte-Code, der vor dem standardmäßigen 4-Byte-ICV eingefügt wird, der beim WEP-Standardverfahren an die 802.11-Nachricht angehängt wird. Dadurch werden Angriffe mit gefälschten Informationen erheblich erschwert. Bei beiden Verfahren zur Integritätsprüfung werden die Werte vom Empfänger berechnet und mit den vom Absender in dem Frame gesendeten Werten verglichen. Wenn die Werte übereinstimmen, ist gewährleistet, dass die Nachricht nicht manipuliert wurde. (*Siehe* WPA, TKIP und ICV).
MTU	Maximum Transmission Unit. Die größte Paketgröße, gemessen in Bytes, die eine Netzwerkschnittstelle konfigurationsgemäß akzeptiert. Nachrichten, die größer als die MTU sind, werden vor dem Senden in kleinere Pakete unterteilt.
MU	Mobile Unit, ein drahtloses Gerät wie zum Beispiel ein Laptop.
Multicast, Broadcast, Unicast	Multicast: Senden einer einzelnen Nachricht an eine ausgewählte Gruppe von Empfängern. Broadcast: Senden einer Nachricht an alle an ein Netzwerk angeschlossenen Empfänger. Unicast: Kommunikation über ein Netzwerk zwischen einem einzelnen Sender und einem einzelnen Empfänger.

Begriff	Definition
Netzmaske	Bei der Verwaltung von Internetsites ist eine Netzmaske eine Folge von Nullen und Einsen, die den Netzwerkabschnitt einer IP-Adresse verbirgt bzw. ausblendet, sodass nur der Hostcomputer-Abschnitt verbleibt. Eine häufig gebrauchte Netzmaske ist 255.255.255.0, die für Class-C-Subnetze (mit bis zu 255 Hosts) verwendet wird. Die ".0" in der Netzmaske "255.255.255.0" lässt zu, dass die Adresse des speziellen Hostcomputers sichtbar ist.
NIC	Network Interface Card (Netzwerkkarte). Eine Erweiterungskarte in einem Computer, die den Computer mit einem Netzwerk verbindet.
NMS	Network Management System. Das System, das zuständig für die Verwaltung eines Netzwerks oder Netzwerkabschnitts ist. Das NMS kommuniziert mit Network Management-Agents, die sich in den verwalteten Knoten befinden.
OFDM	Orthogonal Frequency Division Multiplexing, eine Methode der digitalen Modulation, bei der ein Signal in mehrere Schmalband-Kanäle mit unterschiedlichen Frequenzen unterteilt wird. OFDM entspricht dem herkömmlichen Frequency Division Multiplexing (FDM). Der Unterschied besteht in der Methode, mit der die Signale moduliert und demoduliert werden. Vorrang hat dabei hat die Reduzierung der Interferenz, oder des Nebensprechens, zwischen den Kanälen und Zeichen, die den Datenstrom bilden. Weniger Gewicht wird auf die Perfektionierung einzelner Kanäle gelegt. OFDM wird in Europa für digitale AudioBroadcast-Dienste verwendet. Es wird auch in drahtlosen lokalen Netzwerken (WLANs) verwendet.
OS	Operating System (Betriebssystem).
OSI	Open System Interconnection. Ein ISO-Standard für die weltweite Kommunikation, der eine Netzwerkstruktur für die Implementierung von Protokollen in sieben Schichten definiert. Die Kontrolle wird dabei von einer Schicht zur darunter liegenden nächsten Schicht weitergereicht, beginnend auf einer Station mit der Anwendungsschicht, über die Darstellungsschicht, Sitzungsschicht, Transportschicht, Vermittlungsschicht und Sicherungsschicht bis zur Bitübertragungsschicht, von dort über die Transitsysteme zur nächsten Station, wo dieselbe Hierarchie umgekehrt von unten nach oben durchlaufen wird.

Begriff	Definition
OSI-Schicht 2	Auf der Sicherungsschicht (OSI-Schicht 2) werden Datenpakete in Bits codiert und decodiert. Die Sicherungsschicht ist in zwei Unterebenen aufgeteilt: ● Die Logical Link Control (LLC)-Schicht steuert die Framesynchronisierung, den Datenfluss und die Fehlerüberprüfung. ● Die Media Access Control (MAC)-Schicht steuert, wie ein Computer im Netzwerk auf die Daten zugreift und die Berechtigung zum Übertragen der Daten erhält.
OSI-Schicht 3	Die Vermittlungsschicht (OSI-Schicht 3) stellt Vermittlungs- und Routing-Technologien bereit und richtet logische Pfade ein (als virtuelle Verbindungen bezeichnet), um Daten von Knoten zu Knoten zu übertragen. Zu den Funktionen dieser Schicht gehören Verbindungsaufbau und -abbau, Routing, Adressierung, Netzwerkressourcen-Verwaltung, Fehlerbehandlung, Flusssteuerung und Paketformatierung.
OUI	Organizationally Unique Identifier (verwendet bei MAC-Adressierung).
Paket	Die Dateneinheit, die zwischen einem Ursprung und einem Ziel im Internet oder einem anderen paketvermittelten Netzwerk übertragen wird. Wenn eine Datei im Internet von einem Ort an einen anderen gesendet wird, unterteilt die Transmission Control Protocol (TCP)-Schicht von TCP/IP die Datei in Pakete. Jedes Paket wird einzeln nummeriert und enthält die Internetadresse des Ziels. Die einzelnen Pakete einer bestimmten Datei können auf unterschiedlichen Routen über das Internet übertragen werden. Wenn alle Pakete angekommen sind, werden sie wieder zu der ursprünglichen Datei zusammengefügt (von der TCP-Schicht am empfangenden Ende).
PDU	Protocol Data Unit. Die Protokolldateneinheit ist ein zwischen Protokollcomputern (wie Verwaltungsstationen, SMUX-Peers und SNMP-Agents) ausgetauschtes Datenobjekt, das sowohl Protokollsteuerinformationen als auch Nutzdaten enthält. PDU wird manchmal synonym mit "Paket" verwendet.
PKI	Public Key Infrastructure
PoE	Power-over-Ethernet. Der Power-over-Ethernet-Standard (802.3af) definiert, wie Netzwerkgeräte über eine bestehende Ethernet-Verbindung mit Strom versorgt werden können, sodass keine externe Stromversorgung benötigt wird.
POST	Power On Self Test. Eine von einem Computer durchgeführte Abfolge von Diagnosetests, um zu ermitteln, ob seine Hardware-Systemkomponenten vorhanden und angeschlossen sind. Wenn dies bestätigt wurde, beginnt der Computer mit seinem Bootvorgang.

Begriff	Definition
Push-to-Talk (PTT)	Push-to-Talk (PTT) ist ein Leistungsmerkmal auf drahtlosen Telefonen, mit dem das Gerät im Gegensatz zum normalen Telefonbetrieb wie ein Funksprechgerät in einer Gruppe betrieben werden kann. Damit das PTT-Leistungsmerkmal funktioniert, muss das Netzwerk Multicast-Verkehr zulassen. Ein PTT-Anruf wird initiiert, indem ein Kanal ausgewählt und die Sprechtaste auf dem drahtlosen Telefon betätigt wird. Alle drahtlosen Telefone auf demselben Netzwerk, die den Kanal überwachen, hören die Übertragung. Bei einem PTT-Anruf wird die Taste zum Sprechen gehalten und zum Hören losgelassen.
QoS	Quality of Service. Ein Begriff für eine Reihe von Verfahren, die Anforderungen spezieller Anwendungen intelligent an die verfügbaren Netzwerkressourcen anpassen, wobei Technologien wie Frame Relay, Asynchronous Transfer Mode (ATM), Ethernet- und 802.1-Netzwerke, SONET und IP-vermittelte Netzwerke zum Einsatz kommen. QoS-Leistungsmerkmale verbessern den Netzwerkdienst durch Unterstützung reservierter Bandbreite, Reduzierung von Übertragungsverlusten, Verhindern und Beheben von Netzwerküberlastungen, Formung des Netzverkehrs (Traffic Shaping) und Festlegen von Verkehrsprioritäten im gesamten Netzwerk. Quality-of-Service (QoS): Ein Satz von Service-Anforderungen, der vom Netzwerk beim Transport eines Datenflusses erfüllt sein muss. (RFC2386)
RADIUS	Remote Authentication Dial-In User Service. Ein Authentifizierungs- und Abrechnungssystem, das Benutzername und Kennwort überprüft und den Zugang zu einem Netzwerk autorisiert. Die RADIUS-Spezifikation wird von einer IETF-Arbeitsgruppe bearbeitet (RFC2865 RADIUS, RFC2866 RADIUS Accounting, RFC2868 RADIUS Attributes for Tunnel Protocol Support).
RF	Radio Frequency. Die Frequenz (Funkfrequenz) im elektromagnetischen Spektrum, in der eine Funkübertragung durchgeführt wird. Wenn ein RF-Strom an eine Antenne angelegt wird, entsteht ein elektromagnetisches Feld von Funkwellen, die über den Äther übertragen werden können. Die Frequenzen im elektromagnetischen Spektrum reichen von der extrem tiefen Frequenz (Extremely Low Frequency, ELF) – 30-300 Hz – bis zur extrem hohen Frequenz (Extremely High Frequency, EHF) – 30-300 GHz. Die mittleren Bereiche sind: Low Frequency (LF) – 30-300 kHz, Medium Frequency (MF) – 300-3000 kHz, High Frequency (HF) – 3-30 MHz, Very High Frequency (VHF) – 30-300 MHz, Ultra-High Frequency (UHF) – 300-3000 MHz.

Begriff	Definition
RFC	Request for Comments, eine Serie von Dokumenten über das Internet, werden bei der Internet Engineering Task Force (IETF) eingereicht und erhalten eine RFC-Nummer; RFCs können sich zu einem Internet-Standard entwickeln. Die RFCs werden auf der IETF RFC-Website www.ietf.org/rfc.html katalogisiert und verwaltet.
Roaming	Bei 802.11 erfolgt Roaming, wenn ein drahtloses Gerät (eine Station) sich im selben Extended Service Set (ESS), identifiziert durch seine SSID, von einem Access Point (oder BSS) zu einem anderen bewegt.
RP-SMA	Reverse Polarity-Subminiature Version A, ein Steckertyp, der mit drahtlosen Antennen verwendet wird.
RSN	Robust Security Network. Ein neuer Standard in IEEE 802.11, der Sicherheits- und Datenschutzmechanismen bereitstellt. Das RSN (und das dazugehörige TSN) definieren beide die IEEE 802.1x-Authentifizierung mittels Extensible Authentication Protocol (EAP).
RSSI	Received Signal Strength Indication (im 802.11-Standard)
RTS / CTS	Request To Send (Sendeanforderung), Clear To Send (Sendebereitschaft) (im 802.11-Standard)
Segment	In Ethernet-Netzwerken ein Abschnitt eines Netzwerks, der von Bridges, Routern oder Switches begrenzt wird. Die Unterteilung eines LAN-Segments in mehrere kleinere Segmente ist eine der häufigsten Methoden, um die verfügbare Bandbreite in dem LAN zu erhöhen.
SIAPP	Siemens Inter-Access Point Protocol

Begriff	Definition
SSID	Service Set Identifier Eine aus 32 Zeichen bestehende eindeutige Kennung, die an den Header von über ein WLAN gesendeten Paketen angehängt wird und als Kennwort fungiert, wenn ein drahtloses Gerät versucht, die Verbindung zum Basic Service Set (BSS) herzustellen. Mehrere Basic Service Sets können zu einem logischen WLAN-Segment verbunden werden, das als Extended Service Set (ESS) bezeichnet wird. Die SSID dient zum Identifizieren des ESS. In 802.11-Netzwerken gibt jeder Access Point seine Anwesenheit mehrere Male pro Sekunde bekannt, indem er Beacon-Frames rundsendet, die den ESS-Namen (SSID) tragen. Stationen erkennen APs, indem sie Beacons abhören oder indem sie Probe-Frames senden, um nach einem Access Point mit einer gewünschten SSID zu suchen. Wenn die Station einen Access Point mit passendem Namen findet, sendet sie einen Verbindungsanforderungs-Frame, der die gewünschte SSID enthält. Der Access Point antwortet mit einem Verbindungsantwort-Frame, der ebenfalls die SSID enthält. Einige APs können so konfiguriert werden, dass nicht ihre tatsächliche SSID, sondern eine Broadcast-SSID mit Null-Länge in Beacon-Frames senden. Der Access Point muss in der Probe-Antwort seine tatsächliche SSID zurückgeben.
Subnetze	Teile eines Netzwerks, die das gleiche gemeinsame Adressformat haben. Subnetze in einem TCP/IP-Netzwerk verwenden dieselben ersten drei Zahlensätze (zum Beispiel 198.63.45.xxx), während der vierte Satz zum Identifizieren von Geräten in dem Subnetz dient. Ein Subnetz kann verwendet werden, um die Bandbreite im Netzwerk zu erhöhen, indem das Netz in Segmente unterteilt wird.
Subnetzmaske	(*Siehe* Netzmaske)
SVP	SpectraLink Voice Priority, ein von SpectraLink entwickeltes Protokoll, wird auf Access Points eingesetzt, um die Sprachpriorisierung über ein 802.11-WLAN zu vereinfachen, das Sprachpakete von SpectraLink Wireless-Telefonen transportiert.
Switch	In Netzwerken ein Gerät, das Pakete filtert und zwischen LAN-Segmenten weiterleitet. Switches arbeiten auf der Sicherungsschicht (Schicht 2) und manchmal auf der Vermittlungsschicht (Schicht 3) des OSI-Referenzmodells und unterstützen daher alle Paketprotokolle. Ein LAN, auf dem Switches zum Verbinden von Segmenten genutzt werden, wird als Switched LAN oder, im Fall eines Ethernet-Netzwerks, als Switched Ethernet-LAN bezeichnet.

Begriff	Definition
TCP / IP	Transmission Control Protocol. TCP ist zusammen mit IP (Internetprotokoll) das grundlegende Kommunikationsprotokoll im Internet. Das Transmission Control Protocol ist zuständig für die Aufteilung einer Nachricht oder Datei in kleinere Pakete, die über das Internet gesendet werden und von einer TCP-Schicht empfangen werden, die die Pakete wieder zur Originalnachricht zusammensetzt. Das Internetprotokoll verwaltet den Adressabschnitt jedes Pakets, sodass es an das richtige Ziel gelangt. TCP/IP verwendet das Client/Server-Kommunikationsmodell, bei dem ein Computernutzer (ein Client) einen Dienst anfordert (zum Beispiel das Senden einer Webseite), der dann von einem anderen Computer (einem Server) im Netzwerk bereitgestellt wird.
TFTP	Trivial File Transfer Protocol. Ein Internet-Softwareprogramm zur Übertragung von Dateien, das einfacher verwendbar als das File Transfer Protocol (FTP) ist, aber weniger leistungsfähig. Es wird verwendet, wenn Benutzerauthentifizierung und Verzeichnis-Sichtbarkeit nicht erforderlich sind. TFTP verwendet nicht das Transmission Control Protocol (TCP), sondern das User Datagram Protocol (UDP). TFTP wird im Request For Comments (RFC) 1350 formal beschrieben.
TKIP	Temporal Key Integrity Protocol (TKIP) ist eine Erweiterung des WEP-Verschlüsselungsverfahrens, bei der über einen Satz von Algorithmen eine Rotation der Sitzungsschlüssel erfolgt. Die erweiterte Verschlüsselung durch TKIP beinhaltet eine Schlüsselmischfunktion pro Paket, einen Message Integrity Check (MIC), einen erweiterten Initialisierungsvektor (IV) mit Sequenzregeln und eine Schlüsselwechselfunktion. Die Chiffrierschlüssel werden nach dem Schlüsselwechsel-Intervall (entweder ein bestimmter Zeitraum oder eine bestimmte Anzahl übertragener Pakete) automatisch geändert und zwischen Geräten authentifiziert.
ToS / DSCP	ToS (Type of Service) / DSCP (Diffserve Codepoint). Das ToS/DSCP-Feld im IP-Header eines Frames wird von Anwendungen genutzt, um die Priorität und Service-Qualität (QoS) für jeden Frame anzugeben. Die Service-Qualität wird anhand eines Satzes von Service-Parametern bestimmt, die zwischen den drei Faktoren geringe Verzögerung, hohe Zuverlässigkeit und hoher Durchsatz abwägen. Durch die Verwendung von Service-Parametern können sich die Service-Kosten erhöhen.

Begriff	Definition
TSN	Transition Security Network. Ein Teil des Robust Security Network (RSN), der eine erweiterte Sicherheitslösung für Legacy-Hardware bietet. Die Wi-Fi Alliance hat eine auf TSN basierende Lösung mit der Bezeichnung Wireless Protected Access (WPA) übernommen. RSN und TSN definieren beide die IEEE 802.1x-Authentifizierung mittels Extensible Authentication Protocol (EAP).
Tunnelling	Tunnelling (oder Verkapselung) ist eine Technik, die es einem Netzwerk ermöglicht, seine Daten über die Verbindungen eines anderen Netzwerks zu senden. Beim Tunnelling werden Pakete eines Netzwerkprotokolls in Pakete verkapselt, die vom zweiten Netzwerk transportiert werden. Das empfangende Gerät entkapselt dann die Pakete und leitet sie in ihrem ursprünglichen Format weiter.
U-NII	Unlicensed National Information Infrastructure. U-NII soll drahtlose Netzwerkverbindungen über kurze Distanz, mit hoher Geschwindigkeit und zu günstigen Kosten bereitstellen und besteht aus drei 100-MHz-Frequenzbändern im 5-GHz-Band: 5,15–5,25 GHz (nur in Innenräumen), 5,25–5,35 GHz und 5,725–5,825 GHz. Die drei Frequenzbänder wurden im Jahr 1997 von der US-Regulierungsbehörde für Telekommunikation (FCC) freigehalten, ursprünglich zu dem Zweck, Schulen die drahtlose Verbindung zum Internet zu ermöglichen. U-NII-Geräte erfordern keine Lizenzierung.
UDP	User Datagram Protocol. Ein verbindungsloses Protokoll, das wie TCP auf IP-Netzwerke aufsetzt. UDP/IP bietet eine direkte Methode zum Senden und Empfangen von Paketen über ein IP-Netzwerk, stellt aber im Gegensatz zu TCP/IP sehr wenige Fehlerbehebungs-Dienste bereit. Es wird primär für das Broadcasting von Nachrichten über ein Netzwerk verwendet.
URL	Uniform Resource Locator. Die eindeutige globale Adresse von Ressourcen oder Dateien im World Wide Web. Der URL enthält den Namen des Protokolls, das für den Zugriff auf die Dateiressource verwendet wird, die IP-Adresse oder den Domänennamen des Computers, auf dem sich die Ressource befindet, und einen Pfadnamen – eine hierarchische Beschreibung des Standorts der Datei auf diesem Computer.
Verbindung	Eine Verbindung zwischen einem drahtlosen Gerät und einem Access Point.

Begriff	Definition
VLAN	Virtual Local Area Network. Ein Netzwerk von Computern, die sich verhalten, als wären sie über dieselbe Verkabelung verbunden, obwohl sie sich physikalisch auf unterschiedlichen Segmenten eines LAN befinden können. VLANs sind nicht mittels Hardware, sondern mittels Software konfiguriert, wodurch sie extrem flexibel sind. Wenn ein Computer physikalisch an einen anderen Standort verschoben wird, kann er auf demselben VLAN bleiben, ohne dass die Hardware neu konfiguriert werden muss. Der Standard ist definiert in IEEE 802.1Q - Virtuelle LANs, der sinngemäß aussagt: "IEEE 802-LANs aller Typen können über Media Access Control (MAC)-Bridges, wie in ISO/IEC 15802-3 spezifiziert, miteinander verbunden werden. Dieser Standard definiert die Verwendung von VLAN-Bridges, die die Definition, den Betrieb und die Verwaltung von VLAN-Topologien in einer Bridged LAN-Infrastruktur ermöglichen."
VoIP	Voice Over Internet Protocol. Ein Verfahren der Internet-Telefonie. Bei VoIP wird eine Sprachübertragung in mehrere Pakete unterteilt, die den effizientesten Pfad durch das Internet nehmen und an ihrem Ziel wieder zusammengesetzt werden.
VPN	Virtual Private Network. Ein privates Netz, das eingerichtet wird, indem Knoten über öffentliche Leitungen verbunden werden. Diese Systeme verwenden Verschlüsselung und andere Sicherheitsmechanismen, um sicherzustellen, dass nur autorisierte Benutzer Zugang zum Netzwerk haben und Daten nicht abgehört werden können.
WEP	Wired Equivalent Privacy. Ein im 802.11b-Standard definiertes Sicherheitsprotokoll für drahtlose lokale Netzwerke (WLANs). WEP schützt die Vertraulichkeit von Daten, die per Funk von einem Endpunkt zu einem anderen übertragen werden, durch verschiedene Verschlüsselungsmechanismen.
Wi-Fi	Wireless Fidelity. Ein Begriff zur Bezeichnung eines auf dem 802.11-Standard basierenden Netzwerks, zum Beispiel ein 802.11a-, 802.11b-, Dual-Band-Netzwerk etc. Der Begriff bezieht sich auf die Wi-Fi Alliance, ein 1999 gegründetes gemeinnütziges internationales Industriekonsortium, das sich die Förderung des WLAN-Standards IEEE 802.11 und die Zertifizierung standardkompatibler Produkte zum Ziel gesetzt hat.

Begriff	Definition
WINS	Windows Internet Naming Service. Ein System der Namensauflösung, das die mit einem bestimmten Computer im Netzwerk verbundene IP-Adresse ermittelt. WINS unterstützt Windows-basierte Client- und Servercomputer im Netzwerk und kann für andere Computer mit speziellen Anordnungen Namensauflösung bereitstellen. WINS unterstützt dynamische Adressierung (DHCP) über eine verteilte Datenbank, die automatisch mit den Namen derzeit verfügbarer Computer und der jedem einzelnen Computer zugewiesenen IP-Adresse aktualisiert wird. Ein alternatives System für die Namensauflösung bei Netzwerkcomputern mit fester IP-Adresse ist DNS.
WLAN	Wireless Local Area Network.
WMM	Wi-Fi Multimedia (WMM) ein von der Wi-Fi Alliance zertifizierter Standard, der Multimedia-Erweiterungen für Wi-Fi-Netzwerke bereitstellt, die die Audio-, Video- und Sprachqualität von Anwendungen verbessern. Dieser Standard ist konform mit den IEEE 802.11e Quality of Service (QoS)-Erweiterungen für 802.11-Netzwerke. WMM bietet priorisierten Medienzugriff, indem die Zeit zwischen der Übertragung von Paketen bei Datenverkehr mit höherer Priorität verkürzt wird. WMM basiert auf der Enhanced Distributed Channel Access (EDCA)-Methode.
WPA	Wireless Protected Access oder Wi-Fi Protected Access. Eine von der Wi-Fi Alliance übernommene Sicherheitslösung, die die WEP-Basisverschlüsselung um Authentifizierung erweitert. Für die Authentifizierung definiert WPA die IEEE 802.1x-Authentifizierung mittels Extensible Authentication Protocol (EAP). Für die Verschlüsselung verwendet WPA das TKIP-Verfahren, bei dem zunächst ein gemeinsamer Schlüssel zwischen Geräten genutzt und dann der Chiffrierschlüssel für jedes Paket geändert wird. Es kann auch Zertifikatsauthentifizierung verwendet werden. Teil des Verschlüsselungsverfahrens sind auch 802.1x-Standards für dynamische Schlüsselverteilung und Message Integrity Check – MIC oder "Michael". Für WPA müssen alle Computer und Geräte mit WPA-Software ausgerüstet sein.

Begriff	Definition
WPA-PSK	Wi-Fi Protected Access mit Preshared Key, ein spezieller WPA-Modus für Benutzer ohne einen Enterprise-Authentifizierungsserver. Stattdessen wird für die Authentifizierung ein Preshared Key verwendet. Der PSK ist ein gemeinsames Kennwort (Passphrase), das sowohl im Wireless Access Point oder Router als auch in den WPA-Clients eingegeben werden muss. Dieser Preshared Key sollte eine zufällige Folge von Zeichen (mindestens 20 Zeichen lang) oder Hexadezimalstellen (Zahlen 0-9 und Buchstaben A-F, mindestens 24 Stellen lang) sein. Nach der ersten Authentifizierung durch das gemeinsame Kennwort übernimmt das Temporal Key Integrity Protocol (TKIP) die Verschlüsselung und den automatischen Schlüsselwechsel (Rekeying).

A Anhang: Protokollcodes und -meldungen

Nachfolgend sind die vom Standalone Access Point bereitgestellten Protokollcodes und -meldungen aufgelistet.

Ereig-niscode (1 Byte)	BOF-Protokollmeldung	Kommentare
1	Neustart verursacht durch "Stromausfall" / "Watchdog-Zeitüberschreitung" / "Programmabsturz" / "CLI-Befehl." / ...	Ausgabe des Grundes für Access Point-Neustart
2	Vulnerable-Time gestartet nach "2" Unterbrechungen	Start der Vulnerable-Time, mit vorangegangener Stromunterbrechung während 2 aufeinander folgender Vulnerable-Times
3	Vulnerable-Time ohne Unterbrechungen beendet	Ende der Vulnerable-Time
4	Konfiguration durch Hardware-Reset auf Standardwerte zurückgesetzt	
5	Cluster-VNS1-Status geändert in "Master" / "Slave" / "Register"	Wichtige SIAPP-Zustandsänderung
6	Slave AP mit IP "10.2.102.10" und MAC "00-0F-C8-F0-1A-E6" im Cluster-VNS1 akzeptiert	Master meldet, dass neuer Slave akzeptiert wurde
7	Slave AP mit IP "10.2.102.10" und MAC "00-0F-C8-F0-1A-E6" aus Cluster-VNS1 entfernt	Master meldet, dass Slave entfernt wurde
8	Client "00-0F-DD-F0-1A-E6" mit VNS1 BSSID "00-0F-C8-F0-1A-E8" verbunden	
9	Verbindung von Client "00-0F-DD-F0-1A-E6" mit VNS1 BSSID "00-0F-C8-F0-1A-E8" aufgehoben	
10	(Wieder-)Verbindung von Client "00-0F-DD-F0-1A-E6" von VNS1 BSSID "00-0F-C8-F0-1A-E8" verweigert	
11	Client "00-0F-DD-F0-1A-E6" mit VNS1 BSSID "00-0F-C8-F0-1A-E8" auf diesem Access Point wiederverbunden von BSSID "00-0F-C8-F0-1A-D0"	

Ereig-niscode (1 Byte)	BOF-Protokollmeldung	Kommentare
12	Client "00-0F-DD-F0-1A-E6" von VNS1 BSSID "00-0F-C8-F0-1A-E8" auf diesem Access Point zu BSSID "00-0F-C8-F0-1A-D0" verschoben	
13	Benutzer "admin" erfolgreich angemeldet	
14	Anmeldung von Benutzer "admin" verweigert	
15	Kennwort für Benutzer "admin" erfolgreich geändert	
16	Konfiguration erfolgreich geändert	
17	Konfiguration erfolgreich heruntergeladen	Massenkonfiguration heruntergeladen
18	Konfiguration durch Software-Reset auf Standardwerte zurückgesetzt	
19	Firmware-Upgrade erfolgreich	
20	BootROM-Upgrade erfolgreich	
21	Nicht flüchtiges Protokoll gelöscht	
22	Debug-Info: "SIAPP 87 R0->M2"	
23	Beginn der Radarstörungsprüfung auf Kanal 5300	
24	Ende der Radarstörungsprüfung auf Kanal 5300	
25	Radar geortet. Auf automatische Kanalauswahl umschalten	
26	Automatische Kanalauswahl hat Kanal 5300 gefunden	
27	AP-Absturz hat den Grenzwert 4x erreicht	

Tabelle 14 Protokollcodes und -meldungen

B Anhang: Unterstützte Standards

B.1 RFC-Liste

Nachfolgend sind die Request for Comments (RFC)-Standards der Internet Engineering Task Force (IETF) aufgelistet, die vom Standalone Access Point unterstützt werden.

Die Request for Comments, eine Serie von Dokumenten über das Internet, werden bei der Internet Engineering Task Force (IETF) eingereicht und erhalten eine RFC-Nummer; RFCs können sich zu einem Internet-Standard entwickeln. Die RFCs werden auf der IETF RFC-Website www.ietf.org/rfc.html katalogisiert und verwaltet.

RFC-Nummer	Titel
RFC 791	IPv4
RFC 1812	Minimale Router-Anforderungen
RFC 793	Transport Control Protocol (TCP)
RFC 768	User Datagram Protocol (UDP)
RFC 792	Internet Control Message Protocol (ICMP)
RFC 826	Address Resolution Protocol (ARP)
RFC 2131	Dynamic Host Configuration Protocol (DHCP)
RFC 1155	Struktur und Identifizierung von Management-Informationen für TCP/IP-basierte Internets.
RFC 959	File Transfer Protocol (FTP)
RFC 2616	Das Hypertext Transfer Protocol (HTTP)

Tabelle 15 Liste der vom Standalone Access Point unterstützten RFCs

B.2 Liste der 802.11-Standards

Ebenfalls unterstützt werden die unten aufgelisteten IEEE 802.11-Standards:

Standard	Name	Kommentar
802,11	MAC- und PHY-Spezifikationen für drahtloses LAN	
802.11a	Drahtloses LAN	High-Speed-Bitübertragungsschicht im 5-GHz-Band
802.11b	Drahtloses LAN	High-Speed-Bitübertragungsschicht im 2,4-GHz-Band
802.11d	802.11-Erweiterungen für den Betrieb in zusätzlichen Regulatory Domains	
802.11g	Drahtloses LAN	Zusätzliche Erweiterungen im 2,4-GHz-Band mit hoher Datenrate
802.11i	WLAN-Sicherheit und Bereitstellung besserer Netzwerk-Zugangssteuerung	
802.11e	MAC-Erweiterungen für QoS (Zukunft)	
802.3af	DTE-Stromversorgung über MDI (Power-over-Ethernet)	
802,3	CSMA/CD (Ethernet)	
802.3i	10Base-T	
802.3u	100Base-T	
802.3x	Vollduplex	
802.1d	MAC-Bridges	

Tabelle 16 Liste der unterstützten 802.11-Standards

Stichwörter

Zahlen

802.11e 48

A

Access Point
- anmelden 58
- Anschlüsse 52
- Benutzeroberfläche 57
- konfigurieren 67
- Stromversorgung 52

Access Point Installation 51
Access Point Komponenten 46
Access Point Leistungsmerkmale 45
Access Point Vorteile 46
Administrator 57

B

Benutzeroberfläche 57
Benutzertypen 57
Benutzerzustände 57
BootROM 100

C

Cluster 48

D

Diffserve Codepoint (DSCP) 48

F

Firmware
- herunterladen 61

K

Kennwörter
- ändern 60
- Standard 57

Konfiguration
- BootROM aktualisieren 100
- speichern 96
- verwalten 96

L

LAN-Einstellungen
- konfigurieren 67

LED-Status 53

M

Menü
- Administrator 57
- Standardbenutzer 58

N

Netzwerksicherheit 47

P

Power-over-Ethernet (PoE) 52
- PoE-Injector hinzufügen 52

Q

QoS
- VNS 48

Quality of Service (QoS) 48

S

Secure Inter-Access Point Protocol (SIAPP) 48
Standardbenutzer 58
Stromversorgung über AC-Adapter (externes Netzteil) 52

T

Type of Service (IP ToS) 48

V

Verschlüsselungsverfahren 47
VNS 84
- Funkfrequenz konfigurieren 86
- konfigurieren 84
- QoS konfigurieren 91
- Sicherheit konfigurieren 88

Vulnerable-Time-Intervall 53, 54

W

werkseitige Standardeinstellungen
- wiederherstellen 54
- zurücksetzen auf 54

Wi-Fi Multimedia (WMM) 48
WLAN-Einstellungen
  802.11a, erweiterte Konfiguration 79
  802.11b/g, erweiterte Konfiguration 74
  Filter konfigurieren 73
  konfigurieren 71
  QoS konfigurieren 82

Z

Zufallsverzögerung 53, 54

www.siemens.de/hipath

Hofmannstraße 51 • D-81359 München
Bestell-Nr.: A31003-W1110-U100-4-19
Liefermöglichkeiten und technische Änderungen vorbehalten.